Голові разової спеціалізованої
вченої ради ДФ 20.051.242
Карпатського національного
університету імені Василя Стефаника,
доктору політичних наук, професору,
професору кафедри політичних наук
Климончуку Василю Йосифовичу
(76018, м. Івано-Франківськ,
вул. Шевченка, 57)

**РЕЦЕНЗІЯ**

кандидата політичних наук, доцента кафедри політичних наук
Карпатського національного університету імені Василя Стефаника
**Мадриги Тетяни Богданівни**
на дисертаційну роботу Савлюка Михайла Івановича
**«Загрози інформаційній безпеці в соціальних мережах під час Війни за Незалежність України»**
подану на здобуття наукового ступеня доктора філософії
з галузі знань 05 Соціальні та поведінкові науки за спеціальністю 052
Політологія

**Актуальність дисертаційного дослідження.** Дисертація Савлюка М. І. присвячена актуальній проблематиці у контексті сучасних безпекових і політичних викликів. Цифровізація комунікацій перетворила соціальні мережі на потужний інструмент впливу на суспільну свідомість, політичні процеси та національну ідентичність. Платформізація публічної сфери змінила традиційні моделі політичної комунікації: сьогодні порядок денний значною мірою формується не редакціями та інституціями, а алгоритмами розподілу уваги, лідерами думок і анонімними мережевими структурами, що робить суспільство водночас більш залученим до політики та більш вразливим до маніпулятивних впливів.

В умовах повномасштабної російської агресії інформаційний простір став повноцінним полем бою, де дезінформація, інформаційно-психологічні операції

та кіберзагрози використовуються для підриву стійкості держави й суспільства. Український досвід 2014 – 2025 рр. – від інформаційного супроводу анексії Криму до кампаній періоду повномасштабного вторгнення – демонструє, що загрози в соціальних мережах мають системний, скоординований і довгостроковий характер, а їхня нейтралізація потребує не ситуативних реакцій, а цілісної державної політики та розвиненої інституційної інфраструктури.

Тому політологічне осмислення загроз інформаційній безпеці в соціальних мережах та обґрунтування механізмів протидії їм має не лише теоретичне, а й безпосереднє практичне значення. Обрана здобувачем тема є актуальною, своєчасною та узгоджується з пріоритетами національної безпеки України; вона корелює із завданнями, окресленими у стратегічних документах держави у сферах інформаційної безпеки та кібербезпеки, і водночас заповнює відчутну прогалину у вітчизняному політологічному дискурсі, де соціальні мережі як окреме середовище безпекових загроз досі досліджувалися здебільшого фрагментарно.

**Зв'язок роботи з науковими програмами, планами, темами.** Тему дисертаційного дослідження затверджено Вченою радою Прикарпатського національного університету імені Василя Стефаника (протокол № 09 від 01 листопада 2022 р.). Дисертаційне дослідження здійснене на кафедрі політичних наук у рамках наукової теми кафедри «Трансформація сучасної політичної системи України: внутрішньополітичні виклики та зовнішні впливи» (номер державної реєстрації 0117U004396).

**Ступінь обґрунтованості та достовірність наукових положень, висновків і рекомендацій.** Наукові положення, висновки та рекомендації, сформульовані в дисертації, характеризуються високим рівнем обґрунтованості й достовірності, що забезпечено насамперед коректною постановкою дослідницької мети та завдань. Метою роботи є всебічний аналіз загроз інформаційній безпеці в соціальних мережах в умовах Війни за Незалежність України та обґрунтування механізмів захисту й підвищення стійкості інформаційного простору держави на основі українського та міжнародного досвіду. *Об'єктом* дослідження визначено особливості формування та

функціонування інформаційної безпеки України в умовах зовнішніх загроз і впливів, а *предметом* – загрози інформаційній безпеці України в соціальних мережах в умовах гібридної війни, механізми та закономірності їх виявлення й нейтралізації. Така конфігурація мети, об'єкта і предмета є внутрішньо узгодженою й задає чітку логіку розгортання дослідження від теоретико-понятійного рівня до прикладних кейсів і рекомендацій.

Методологічний інструментарій дисертації відповідає поставленим завданням, а вибір кожного методу зумовлений його функцією в архітектурі дослідження. Системний підхід дав змогу розглянути інформаційну безпеку як цілісний багаторівневий феномен у єдності її політичних, правових, технологічних і соціокультурних вимірів; компаративний аналіз застосовано для зіставлення українського та зарубіжного досвіду протидії інформаційним загрозам; документальний аналіз нормативно-правової бази забезпечив оцінювання регуляторних засад і практик державного реагування у сфері інформаційної безпеки; контент-аналіз та івент-аналіз використано для опрацювання емпіричного матеріалу соціальних мереж і хронології інформаційних кампаній; метод кейс-стаді – для поглибленого вивчення ключових епізодів інформаційного впливу на Україну у 2014–2025 рр.; SWOT-аналіз – для оцінювання сильних і слабких сторін національної системи інформаційної безпеки, можливостей та загроз її розвитку; елементи моделювання і прогнозування – для обґрунтування інституційної моделі протидії та окреслення перспективних сценаріїв.

Достовірність результатів підтверджується репрезентативністю джерельної бази, яка налічує 386 позицій та охоплює нормативно-правові акти України й інших держав, стратегічні документи у сферах національної та інформаційної безпеки, праці вітчизняних і зарубіжних дослідників, аналітичні матеріали профільних інституцій, а також емпіричні матеріали українського інформаційного простору 2014–2025 рр. Це забезпечує високу аналітичну якість та практичну спрямованість дослідження.

Логіка дослідження підпорядкована послідовному розв'язанню взаємопов'язаних завдань: з'ясувати сутність, структуру та функції

інформаційної безпеки як складника національної безпеки; систематизувати наукові підходи й методи її дослідження; проаналізувати нормативно-правову базу забезпечення інформаційної та кібербезпеки України; розкрити роль соціальних мереж як інструменту стратегічного впливу, визначити їхні функціональні характеристики, уразливості та роль у формуванні інформаційного порядку денного в умовах конфлікту; охарактеризувати інформаційно-психологічні операції та технічні інструменти ведення гібридної війни; здійснити аналіз ключових кейсів інформаційного впливу на Україну у 2014–2025 рр.; узагальнити український і світовий досвід протидії інформаційним загрозам, визначити ефективні практики, інституційні моделі та інструменти підвищення стійкості інформаційного простору. Кожному поставленому завданню відповідає окремий структурний компонент дисертації, а сформульовані висновки узгоджуються з визначеними завданнями, що свідчить про логічну цілісність і завершеність дослідження.

**Наукова новизна одержаних результатів.** Результати дослідження характеризуються належним рівнем наукової новизни, яка підтверджується змістом роботи та опублікованими працями здобувача. *Уперше* комплексно досліджено сучасні загрози інформаційній безпеці України в соціальних мережах як складник гібридної війни: визначено їхню політичну природу, механізми продукування й поширення та безпекові наслідки для держави й суспільства; розроблено та обґрунтовано механізм інституційної взаємодії у сфері протидії загрозам у соціальних мережах, що враховує багаторівневість суб’єктів (державні органи, сектор безпеки й оборони, медіа, громадянське суспільство, міжнародні партнери, платформи) та потребу гнучкої координації в умовах швидкозмінних інформаційних кампаній; здійснено типологізацію загроз у соціальних мережах та визначено індикатори їх виявлення; проаналізовано ключові кейси інформаційного впливу на Україну у 2014–2025 рр. із застосуванням SWOT-аналізу та елементів прогнозування до сфери інформаційної безпеки в соціальних мережах.

*Удосконалено* теоретико-методологічні засади аналізу інформаційної безпеки в умовах диджиталізації та платформізації політичних комунікацій, що

дало змогу точніше розкрити специфіку загроз у соціальних мережах як окремого сегмента інформаційного простору, а також категоріально-понятійний апарат дослідження через уточнення змісту й співвідношення понять «інформаційна безпека» – «інформаційна агресія» – «ІПСО» – «дезінформація» – «стратегічні комунікації» – «стійкість інформаційного простору»; удосконалено підхід до аналізу інституційних чинників інформаційно-безпекової політики України шляхом функційного структурування завдань у сфері соціальних мереж за напрямами моніторингу, превенції, реагування, кризових комунікацій, міжвідомчої координації, взаємодії з цифровими платформами та громадянським суспільством тощо.

*Набули подальшого розвитку* положення про роль соціальних мереж як інструменту стратегічного впливу в умовах гібридної війни; значення інституційної спроможності держави у протидії інформаційним загрозам у соціальних мережах; поєднання реактивних і проактивних підходів у політиці інформаційної безпеки; механізми міжнародної взаємодії у сфері протидії дезінформації та інформаційно-психологічним операціям як чинник посилення національної стійкості України (с. 29-31).

Окремо варто відзначити емпіричну верифікацію теоретичних положень дисертації. Аналіз конкретних кейсів інформаційного впливу – від інформаційного супроводу анексії Криму та війни на Донбасі до масштабних дезінформаційних кампаній періоду повномасштабного вторгнення – здійснено на основі задокументованих матеріалів українського інформаційного простору, офіційних повідомлень профільних державних інституцій та аналітичних звітів дослідницьких центрів.

Поєднання якісних і кількісних методів опрацювання матеріалу, тріангуляція джерел та зіставлення українського досвіду з міжнародною практикою забезпечують надійність емпіричного підґрунтя роботи й переконливість зроблених автором узагальнень.

**Теоретичне та практичне значення результатів.** Теоретичне значення дисертації полягає в розвитку політологічних уявлень про інформаційну безпеку як соціально-політичного феномену і складника національної безпеки, у

концептуалізації соціальних мереж як середовища стратегічного впливу в умовах гібридних конфліктів та в уточненні категорійно-понятійного апарату відповідної дослідницької галузі. Запропоновані здобувачем підходи формують теоретичне підґрунтя для подальших досліджень інформаційного протиборства, цифрової пропаганди та політики платформ у воєнний і повоєнний періоди.

Особливу прикладну цінність мають положення дисертації щодо інституційної моделі взаємодії суб'єктів протидії інформаційним загрозам та рекомендації з підвищення стійкості інформаційного простору. Вони можуть бути безпосередньо використані під час удосконалення стратегічних і програмних документів держави у сферах інформаційної безпеки та стратегічних комунікацій, у плануванні діяльності профільних інституцій сектору безпеки й оборони, а також у розробленні освітніх програм із медіаграмотності для різних цільових аудиторій.

Практичне значення визначається можливістю використання сформульованих висновків і рекомендацій у діяльності органів публічної влади та сектору безпеки й оборони України, зокрема суб'єктів забезпечення інформаційної безпеки та стратегічних комунікацій; в удосконаленні державної інформаційно-безпекової політики щодо соціальних мереж; у роботі інститутів громадянського суспільства й медіа, що протидіють дезінформації; а також у навчальному процесі закладів вищої освіти під час викладання дисциплін за спеціальностями «Політологія», «Національна безпека», «Міжнародні відносини», «Журналістика» та спорідненими напрямами підготовки.

**Характеристика основних положень роботи.** Дисертаційна робота є логічною за своєю структурою та відповідає вимогам щодо обсягу, який зумовлений метою й завданнями дослідження.

У першому розділі **«Теоретико-методологічні дослідження інформаційної безпеки»** (с. 34-87) розкрито теоретико-методологічні засади дослідження: з'ясовано сутність інформаційної безпеки, її структурні компоненти та функції як складника національної безпеки (с. 35–54); систематизовано основні теоретичні підходи та обґрунтовано методологічний інструментарій дослідження (с. 55–72); проаналізовано нормативно-правову

базу забезпечення інформаційної та кібербезпеки України (с. 73–87). Доречним є розуміння автором інформаційної безпеки не лише як сфери технічного захисту інформації, а як комплексного політико-соціального явища, що охоплює технологічний, когнітивно-психологічний, інституційно-політичний, соціальний та міжнародний виміри (с. 20–21, 35–54). На позитивну оцінку заслуговує застосування системного підходу, що дало змогу здобувачеві розглядати інформаційну безпеку через взаємозв'язок нормативно-правової бази, інституційної архітектури, механізмів координації, комунікаційних практик, технологічних чинників і зовнішніх впливів (с. 64–66). Слушним є і акцент здобувача на тому, що інформаційна безпека в політологічному вимірі не обмежується суто технічним захистом інформації, а охоплює політичні, соціальні та правові аспекти управління інформаційними процесами, а також здатність держави й суспільства зберігати суб'єктність у власному інформаційному просторі.

Другий розділ **«Особливості та технології ведення гібридної війни в соціальних мережах»** (с. 88–143) присвячено аналізу соціальних мереж як середовища реалізації стратегічного інформаційного впливу та розкрито їхню роль у сучасній гібридній війні. Послідовно проаналізовано функціональні характеристики й амбівалентний мобілізаційний потенціал соціальних мереж (с.88–102), інформаційно-психологічні операції, їхні цілі, технології та механізми маніпулятивного впливу (с. 103–123), а також кіберзагрози й технічні інструменти гібридної війни (с. 124–143). Важливим результатом розділу є систематизація таких інструментів, як автоматизовані бот-мережі, фейкові акаунти (sockpuppet), технології маніпуляції контентом і координована неавтентична поведінка. На позитивну оцінку заслуговує те, що здобувач не обмежується характеристикою технологічного інструментарію, а розглядає його у взаємозв'язку з політичними цілями агресора та загальною стратегією гібридного впливу на Україну. Такий підхід дозволяє показати, що інформаційні та кіберінструменти виступають не самостійними проявами загроз, а складовими комплексної стратегії гібридного впливу, спрямованої на дестабілізацію

політичної системи, підрив довіри до державних інституцій та послаблення суспільної стійкості.

У третьому розділі **«Механізми захисту та підвищення стійкості інформаційного простору в умовах гібридної війни»** (с. 144–208) дослідження набуває виразного прикладного характеру. У підрозділі 3.1 (с. 144–176) узагальнено український і зарубіжний досвід протидії інформаційним загрозам у соціальних мережах, тоді як у підрозділі 3.2 (с. 177–208) здійснено аналіз ключових кейсів інформаційного впливу на Україну впродовж 2014–2025 рр. Вагомим результатом є простеження еволюції інформаційної агресії – від переважно локалізованих операцій 2014–2015 рр. до масштабного інформаційного наступу в умовах повномасштабного вторгнення, а також виокремлення стійких наративних конструкцій, спрямованих на підрив української державності та її легітимності. Значну увагу приділено аналізу діяльності українських інституцій протидії дезінформації та кіберзагрозам і зіставленню вітчизняного досвіду з практиками Фінляндії, Швеції, США, Великої Британії та інших держав. Позитивної оцінки заслуговує обґрунтування необхідності комплексного підходу до зміцнення стійкості інформаційного простору, який поєднує нормативно-правові, інституційні, комунікаційні та освітні інструменти, розвиток спроможностей реагування та міжнародну співпрацю. Запропоновані рекомендації мають практико-орієнтований характер і охоплюють як удосконалення діяльності профільних державних інституцій, так і розвиток суспільної медіаграмотності.

У висновках (с. 209–223) узагальнено результати проведеного дослідження відповідно до поставленої мети та завдань. Логіка викладу дозволяє простежити послідовний перехід від теоретичного осмислення інформаційної безпеки до аналізу конкретних технологій і практик інформаційного впливу та обґрунтування механізмів протидії їм. Особливо вагомими є положення щодо розуміння соціальних мереж як середовища стратегічного впливу, багаторівневого характеру загроз інформаційній безпеці та необхідності поєднання реактивних і проактивних механізмів їх нейтралізації.

**Повнота викладу положень дисертації в наукових публікаціях, зарахованих за темою дисертації.** Детальне ознайомлення з текстом дослідження та опублікованими працями за темою дисертації дозволяє зробити висновок, що основні результати дисертаційного дослідження викладено у наукових публікаціях, у тому числі: у чотирьох статтях у вітчизняних фахових виданнях, та чотирьох працях у збірниках матеріалів всеукраїнських та міжнародних наукових конференцій, в одному періодичному виданні (с. 33–34).

**Відомості про дотримання академічної доброчесності.** Аналіз тексту дисертації свідчить про відсутність ознак академічного плагіату, самоплагіату, фальсифікації та інших порушень, що могло б поставити під сумнів самостійний характер виконання автором наукового дослідження. В роботі дисертантом викладені наукові результати, що отримані ним особисто.

**Дискусійні положення та рекомендації до змісту дисертації.** Позитивно оцінюючи актуальність проведеного дослідження, наукову новизну, обґрунтованість і достовірність отриманих результатів, високий теоретичний рівень і практичну значущість висновків, звертаємо увагу на ряд зауважень, що носять рекомендаційний характер:

1. Попри ґрунтовний аналіз внутрішнього інформаційного простору України та залучення міжнародного досвіду протидії дезінформації й кіберзагрозам, у дисертації дещо меншою мірою представлено зовнішньокомунікаційний вимір інформаційної безпеки держави. Зокрема, додаткової уваги заслуговують механізми протидії російським дезінформаційним наративам, орієнтованим на зарубіжні аудиторії, та роль стратегічних комунікацій України у міжнародному інформаційному просторі. З огляду на транснаціональний характер сучасних інформаційних загроз, поглиблення цього аспекту дало б змогу повніше розкрити взаємозв’язок внутрішнього і зовнішнього вимірів забезпечення інформаційної безпеки України.

2. Позитивно оцінюючи залучення значного міжнародного досвіду протидії дезінформації та кіберзагрозам (на прикладі США, Швеції, Фінляндії) (с. 170-177), варто зазначити, що компаративна складова дослідження могла б

бути посилена шляхом чіткішого визначення критеріїв зіставлення обраних країн. Це дозволило б більш системно обґрунтувати можливості адаптації відповідних практик до українських інституційних і безпекових умов.

3. За належного висвітлення нормативно-правового забезпечення інформаційної та кібербезпеки України та європейського регуляторного досвіду, окремі аспекти правового регулювання діяльності соціальних платформ могли б бути розкриті висвітлені більш ґрунтовно. Зокрема, додаткового уточнення потребують питання відповідальності цифрових платформ, протидії координованій неавтентичній поведінці, прозорості алгоритмічних механізмів поширення контенту та захисту користувачів від маніпулятивних інформаційних впливів. Доцільним було б також чіткіше окреслити можливості адаптації відповідних положень європейського регуляторного досвіду, зокрема Акта про цифрові послуги (Digital Services Act, DSA), що визначає засади відповідальності та підзвітності онлайн-платформ, прозорості алгоритмів і модерації контенту, до українського нормативно-правового та інституційного середовища.

Висловлені зауваження мають рекомендаційний характер, є радше побажаннями щодо продовження наукового пошуку, не торкаються сутності здобутих результатів і не впливають на загальну позитивну оцінку рецензованої роботи.

**Загальний висновок про відповідність дисертації встановленим вимогам.** Дисертаційна робота Савлюка Михайла Івановича «Загрози інформаційній безпеці в соціальних мережах під час Війни за Незалежність України» подана на здобуття наукового ступеня доктора філософії за спеціальністю 052 Політологія є самостійним, завершеним, цілісним науковим дослідженням, яке за актуальністю, науковою новизною, важливістю здобутих результатів, їх обґрунтованістю і вірогідністю, практичним значенням відповідає вимогам наказу Міністерства освіти і науки України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації» (зі змінами), «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету

Міністрів України від 12 січня 2022 р. № 44 (зі змінами від 21.03.2022 р. № 341), не містить ознак порушення академічної доброчесності, а тому її автор, Савлюк Михайло Іванович, заслуговує на присудження наукового ступеня доктора філософії з галузі знань 05 Соціальні та поведінкові науки зі спеціальності 052 Політологія.

**Рецензент:**
кандидат політичних наук, доцент
доцент кафедри політичних наук
Карпатського національного університету
імені Василя Стефаника **Тетяна МАДРИГА**