DOI: https://doi.org/10.37634/efp.2024.12.15
УДК 349+342.1

Михайло Олександрович ***ШЕВЧУК***
к.ю.н., докторант, Хмельницький університет управління та права імені Леоніда Юзькова
ORCID: https://orcid.org/0000-0001-7549-6344
e-mail: m.shevchuk522@gmail.com

АНАЛІЗ ЗОВНІШНІХ ДЖЕРЕЛ ІНФОРМАЦІЙНОЇ НЕБЕЗПЕКИ ДЕРЖАВ

У статті розглядаються зовнішні джерела інформаційних загроз державній безпеці, акцентується увага на діяльності зовнішньополітичних, військових, економічних та розвідувальних структур в інформаційній сфері. Досліджуються сучасні методи кібершпигунства та їх вплив на систему національної безпеки. Аналізуються спільні міжнародні зусилля для протидії цим загрозам і необхідності єдиної глобальної політики для забезпечення інформаційного суверенітету та безпеки. Дослідження сприяє глибшому розумінню того, як інтегровані технологічні та інформаційні інструменти використовуються для впливу на стабільність держави, і підкреслює нагальну потребу в адаптивних і проактивних заходах у цифрову епоху.

Ключові слова: *зовнішні джерела, інформаційна безпека, дезінформація, кіберзагрози, політичний вплив, міжнародні терористичні групи, інформаційні війни*

ВСТУП

Інформаційна безпека є важливим аспектом національної безпеки кожної держави, оскільки сучасні виклики в інформаційній сфері набувають дедалі більшої актуальності. Зовнішні джерела інформаційної небезпеки, до яких належать різноманітні зовнішні загрози, створюють ризики для стабільності політичної, економічної та соціальної ситуації в країні. Діяльність іноземних держав, міжнародних терористичних організацій, а також розвідувальних структур в інформаційному просторі здатна не тільки дестабілізувати внутрішню ситуацію, але й послабити суверенітет держави. Тому аналіз цих загроз є важливою науковою та практичною задачею.

В останні роки численні публікації та дослідження сфокусувалися на темі інформаційних атак, кіберзагроз, інформаційних війн і їх впливу на національну безпеку. Зокрема, важливими є роботи, що стосуються діяльності іноземних держав та неурядових акторів в інформаційному просторі, розроблення механізмів протидії дезінформації, а також аналізу методів інформаційних маніпуляцій. Відомі публікації, що досліджують зовнішні загрози, зокрема відомості про вплив соціальних медіа, кібероперації та технології впливу на громадську думку [1].

Вчені зазначають, що інформаційна безпека держави значно залежить від своєчасного виявлення та нейтралізації зовнішніх загроз, які виникають у інформаційному просторі. Так, В. Горбулін і О. Литвиненко наголошують, що сучасні загрози інформаційній безпеці є частиною гібридних воєн і потребують системного аналізу, інтеграції технологій та міжвідомчої координації.

Подібної думки дотримуються й Т. Кузьо, Є. Магда, О. Бєлікова, які стверджують, що основними інструментами зовнішнього впливу є інформаційні війни, розвідувальні операції та маніпуляції через медійні канали. Зокрема, вони вказують на необхідність розроблення національних стратегій протидії з урахуванням міжнародного досвіду.

Інший аспект досліджень висвітлюють M. Chesser і J. Nye, які акцентують на важливості культурного впливу та «м'якої сили» як складника інформаційної експансії. Вони зазначають, що без розуміння культурно-інформаційної інтеграції вплив зовнішніх акторів залишатиметься неконтрольованим.

Сучасні дослідники зосереджуються на комплексному підході до забезпечення інформаційної безпеки держави, який включає правові, технологічні та культурні аспекти протидії зовнішнім загрозам.

Попри значну кількість досліджень, є невирішені питання із системного аналізу зовнішніх джерел інформаційної небезпеки та їх впливу на національну безпеку. Одним з таких аспектів є недостатня увага до комплексного вивчення ролі іноземних держав у маніпулюванні інформаційним простором та зростання їхнього впливу через культурну експансію.

МЕТА роботи – детальний аналіз зовнішніх джерел інформаційної небезпеки, визначення їхніх основних проявів і наслідків для національної безпеки держави. У роботі розглянуто специфіку діяльності іноземних політичних, військових, економічних та розвідувальних структур, а також їх вплив на інформаційну ситуацію всередині країни.

Для досягнення поставленої мети застосовано методи системного аналізу, компаративного аналізу і контент-аналізу. Системний підхід дає змогу розглядати зовнішні джерела небезпеки в контексті широких міжнародних процесів, а також взаємодії різних акторів, що впливають на інформаційну ситуацію. Компаративний аналіз застосовано для порівняння різних підходів у вивченні зовнішніх загроз та методів їх нейтралізації в наукових публікаціях. Контент-аналіз, зі свого боку, дає змогу оцінити конкретні інформаційні кампанії та стратегії впливу, що застосовуються в інформаційних війнах.

РЕЗУЛЬТАТИ

Основною метою роботи є дослідження зовнішніх джерел інформаційної небезпеки, а також визначення шляхів їх нейтралізації. Важливим завданням є аналіз специфічних зовнішніх загроз, зокрема в контексті діяльності іноземних політичних, військових та розвідувальних структур, міжнародних терористичних груп, а також культурної експансії. Враховуючи наявність недосконалих механізмів протидії зовнішнім загрозам, завдання полягає у визначенні основних стратегій для посилення інформаційної безпеки на національному рівні [2].

Іноземні політичні, військові, економічні та розвідувальні структури активно впливають на інформаційну безпеку інших держав. Їх діяльність включає застосування різних засобів та технологій для досягнення політичних, економічних і стратегічних цілей. Це може проявлятися через маніпулювання інформацією, кібернапади, економічний тиск або дезінформаційні кампанії. Нижче наведено ключові аспекти їх діяльності.

У табл. 1 розглянемо діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері.

Іноземні держави активно застосовують інформаційні операції для впливу на політичні процеси в інших країнах. Це може включати втручання у виборчі кампанії, пропаганду, використання фальшивих новин або навіть організацію протестних рухів.

Приклад: Вибори в США (2016 р.) – росія використовувала соціальні мережі та хакерські атаки, щоб вплинути на виборчі процеси та підтримати кандидатуру Д. Трампа, одночасно дискредитуючи кандидата Г. Клінтон.

Військові аспекти інформаційних операцій є важливою частиною сучасних військових стратегій. Вони включають не лише традиційні військові дії, але й активне застосування інформації та технологій для досягнення стратегічних цілей [3]. Військові структури можуть застосовувати інформаційні операції для впливу на бойовий дух супротивника, дезорієнтації його військ, послаблення інфраструктури та зниження ефективності оборони. Інформаційні операції включають психологічні операції, кібератаки, дезінформаційні кампанії, а також ведення інформаційної війни в глобальному контексті.

Кібероперації – напади на інформаційні системи, зокрема на військову та критичну інфраструктуру, з метою знищення або спотворення важливих даних. Ці операції можуть призводити до відключення електричних мереж, збоїв у комунікаціях, втрати контролю над системами управління.

Психологічні операції (PSYOPS) – це операції, спрямовані на вплив на моральний стан ворога через дезінформацію, пропаганду та маніпуляцію суспільною думкою. Вони можуть включати кампанії, що перекручують реальність або створюють ілюзію переваги в бою.

Дезінформація – спосіб введення супротивника в оману стосовно стану бойових дій або стратегічних рішень. Це може включати фальшиві новини, зловживання соціальними мережами або маніпулювання відео та іншими медіа.

Інформаційна війна – комплекс заходів, спрямованих на створення або підтримку інформаційної переваги у війні. Вона включає не лише знищення або маніпуляцію інформацією супротивника, але й активне формування власної інформаційної позиції.

У табл. 2 розглянемо приклади військових інформаційних операцій.

Військові аспекти інформаційних операцій стали важливим інструментом сучасних конфліктів. Кібероперації, психологічні операції, дезінформація і стратегічна інформаційна війна можуть не лише підривати стабільність держав, але й значно змінювати хід бойових дій. Враховуючи ці фактори, важливо розробляти комплексні стратегії для захисту інформаційної безпеки та протидії впливу зовнішніх акторів на національні інтереси.

Економічний вплив через інформаційні канали є важливим складником сучасної економічної війни. Відомо, що інформація може суттєво впливати на фінансові ринки, економічні рішення, а також на міжнародні економічні відносини. Інформаційні канали використовуються для маніпулювання громадською думкою, створення сприятливого або несприятливого іміджу певної країни чи її економіки, а також для контролю над глобальними економічними процесами [4].

Маніпулювання фінансовими ринками – інформація може використовуватися для впливу на курси валют, акції компаній, фондові ринки. Можливість контролювати або маніпулювати інформацією дає змогу державам або корпораціям отримувати економічні переваги.

Сприяння економічним санкціям – інформаційні канали можуть використовуватись для обґрунтування введення економічних санкцій проти певних держав або компаній. Їх може бути використано для поширення інформації про порушення міжнародних норм, корупційні скандали, порушення прав людини.

Економічний імідж держави – вплив на міжнародну репутацію країни є важливим елементом у сфері міжнародної економіки. Інформаційна кампанія може позитивно або негативно впливати на інвестиційний клімат, а також на зовнішньоекономічні зв'язки.

Пропагування економічних стратегій – інформаційні канали можуть бути використані для просування національних економічних проектів та стратегій на міжнародній арені, таких як ініціативи для залучення інвестицій або просування національних брендів.

У табл. 3 розглянемо приклади економічного впливу через інформаційні канали.

Одним з основних способів економічного впливу через інформаційні канали є маніпулювання фінансивими ринками. Влада або корпорації можуть використовувати інформаційні канали для створення або усунення економічних ризиків, що, зі свого боку, впливає на інвестиційну привабливість певної держави або компанії. Інформація про кризу в банківському секторі, падіння цін на нафту або збільшення боргового навантаження держави може спричинити значне падіння вартості національної валюти або акцій компаній [5].

Інформаційні канали також може бути використано для підтримки введення економічних санкцій або обмежень проти країн, які порушують міжнародні норми. Поширення інформації про порушення прав людини, корупційні схеми або агресивні дії держави може стати підґрунтям для санкцій, що мають на меті ослабити економіку країни, змусивши її змінити політичну або економічну поведінку.

Інформаційний імідж держави є ключовим елементом, який визначає її здатність приваблювати інвестиції та партнерства. Позитивний імідж може сприяти покращенню зовнішньоекономічної діяльності та привабливості для інвесторів, тоді як негативний імідж може призвести до скорочення іноземних інвестицій і зниження економічної співпраці.

Інформаційні канали може бути використано для популяризації економічних стратегій країни на міжнародному рівні. Це може включати інвестиційні проєкти, нові економічні зони або національні бренди, які сприяють покращенню економічного клімату.

Таблиця 1 – **Діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері**

Категорія	Опис діяльності	Приклади
Політичний вплив	використання інформації для маніпулювання політичними процесами в інших країнах (вибори, протестні рухи)	російські впливи на вибори в США (2016 р.), використання соціальних мереж для пропаганди
Військові операції	кібернапади на критичну інфраструктуру, психологічні операції для послаблення супротивника	атаки на енергетичні мережі України під час конфлікту з Росією, психологічні операції в Сирії
Економічний вплив	використання інформаційних каналів для економічного тиску або маніпулювання ринками та цінами	китайська присутність у міжнародних медіа, що підтримує економічні інтереси Пекіна
Розвідувальна діяльність	використання кіберрозвідки для збору інформації, зламу комп'ютерних мереж, викрадення конфіденційних даних	кібернапади групи APT28 (Fancy Bear) на урядові структури в Європі та США

Таблиця 2 – **Приклади військових інформаційних операцій**

Тип операції	Приклад
Кібероперації	атака на енергетичні мережі України (2015 р.) через хакерську групу Sandworm (росія)
Психологічні операції	психологічні операції в Сирії, де з допомогою ЗМІ створювалися фальшиві повідомлення про поразки
Дезінформація	російська пропаганда стосовно «націоналістичних» настроїв в Україні для підриву внутрішньої стабільності
Інформаційна війна	Іракська війна 2003 р.: США активно використовували пропаганду через ЗМІ для підтримки своєї військової операції

Таблиця 3 – **Приклади економічного впливу через інформаційні канали**

Тип економічного впливу	Приклад
Маніпулювання фінансовими ринками	Фінансова криза 2008 року, де інформація про неплатоспроможність деяких банків сприяла падінню акцій і валют
Санкції та економічний тиск	Запровадження санкцій проти Росії після анексії Криму в 2014 році, що супроводжувалося потужною медіакампанією
Економічний імідж держави	Китай активно використовує медіа для популяризації ініціативи «Один пояс, один шлях» для залучення інвестицій
Пропагування економічних стратегій	Пропаганда «Індійської економічної революції» через міжнародні новини, щоб привабити інвесторів і спонсорів

Сучасні технології дають змогу розвідувальним органам не лише збирати дані, але й використовувати їх для маніпуляції суспільною думкою, планування економічних, військових чи політичних операцій.

Основні напрями розвідувальної діяльності в інформаційній сфері.

Кібершпигунство – збір конфіденційної інформації через комп'ютерні мережі.

Аналіз великих даних – використання даних із відкритих і закритих джерел для створення аналітичних прогнозів.

Маніпуляція громадською думкою – вплив на суспільство через дезінформацію.

Контроль медіа та соцмереж – моніторинг і маніпулювання інформаційними потоками.

Кібершпигунство є одним із найбільш поширених напрямків розвідувальної діяльності в інформаційній сфері. Злам інформаційних систем дає змогу отримувати доступ до конфіденційних даних урядів, компаній або окремих осіб. Такі операції часто проводяться із залученням висококваліфікованих хакерів або державних агентств.

У 2016 р. хакери з групи Fancy Bear, які, ймовірно, пов’язані з російськими розвідувальними службами, зламали сервери Демократичної партії США, викравши електронні листи, які згодом оприлюднено.

Розвідувальні служби активно застосовують технології аналізу великих даних для виявлення патернів поведінки, прогнозування подій і вивчення суспільних настроїв. Це дає змогу створювати аналітичні моделі, які застосовуються для впливу на економічні, політичні чи військові рішення.

Компанія Cambridge Analytica використовувала дані мільйонів користувачів Facebook для аналізу їхніх політичних уподобань і створення таргетованих рекламних кампаній [6].

Держави використовують свої ресурси для контролю інформаційних потоків у медіа та соцмережах. Це може включати як блокування небажаної інформації, так і просування вигідного контенту.

У Китаї діє система «Великий брандмауер», яка обмежує доступ до закордонних інформаційних ресурсів і блокує контент, який вважається загрозливим для уряду.

У табл. 4 розглянемо основні технології в розвідувальній діяльності інформаційної сфери.

Розвідувальна діяльність в інформаційній сфері стає все більш складною та технологічно розвиненою. Вона охоплює широкий спектр інструментів – від кіберзламів до маніпуляцій у соцмережах. Така діяльність створює значні виклики для національної безпеки, що вимагає розвитку ефективних механізмів захисту та системи моніторингу інформаційних загроз.

Сучасні інформаційні війни значно посилюються через спільне застосування різних технологій для інтеграції впливу на держави, суспільства та окремі групи. Така інтеграція поєднує кібернетичні, інформаційні, комунікаційні, та штучно-інтелектуальні технології для досягнення стратегічних цілей. Вона дає змогу створювати комплексний вплив, що одночасно охоплює політичну, економічну, соціальну та військову сфери [7].

Спільне застосування технологій включає:

– координацію кібероперацій та інформаційних кампаній;

– застосування штучного інтелекту (ШІ) для аналізу великих обсягів даних та персоналізації впливу;

– розроблення платформ для автоматизації пропаганди та маніпуляції громадською думкою;

– синхронізацію військових, економічних та політичних стратегій через цифрові платформи.

У табл. 5 – основні напрямки інтеграції технологій.

Таблиця 4 – **Основні технології в розвідувальній діяльності інформаційної сфери**

Технологія	Функція	Приклад застосування
Соціальна інженерія	отримання доступу до даних через маніпуляцію людьми	фішинг-атаки на урядовців або корпоративних працівників
Боти та тролі	автоматизоване створення контенту для маніпуляції суспільною думкою	бот-мережі, які поширюють пропаганду під час виборів у різних країнах
Big Data Analytics	аналіз даних для створення прогнозів і планування операцій	використання соцмережевих даних для виявлення протестних настроїв
Deepfake технології	створення відео або аудіо для дезінформації та підриву довіри до особистостей	Deepfake-відео для дискредитації політиків

Таблиця 5 – **Основні напрямки інтеграції технологій**

Напрям	Опис	Приклад
Координація кібероперацій та дезінформації	використання кібернападів для знищення або спотворення даних, одночасно підтримуючи кампанії дезінформації	атака на енергосистему України (2015 р.) разом із пропагандою про неспроможність державного управління
Штучний інтелект (ШІ)	використання алгоритмів ШІ для аналізу даних, прогнозування поведінки людей і створення персоналізованих інформаційних атак	використання ШІ у виборчих кампаніях для таргетованої реклами в США (2016 р.)
Автоматизація пропаганди	застосування ботів та автоматичних систем для поширення фейків та інформації, що маніпулює суспільною думкою	використання ботів у соцмережах для поширення фейкових новин під час Brexit
Інтеграція платформ для комунікації	застосування спільних платформ для обміну даними між військовими, економічними та політичними структурами	використання китайських технологій для синхронізації пропаганди в межах ініціативи "Один пояс, один шлях"

У 2015 р. під час атаки на енергетичну інфраструктуру України, паралельно поширювались фейки про те, що уряд неспроможний забезпечити базові послуги. Це створило паніку та втрату довіри до влади.

Під час президентських виборів у США 2016 р. компанія Cambridge Analytica використовувала дані соцмереж для створення персоналізованої реклами, що впливала на виборців залежно від їхніх інтересів і політичних уподобань.

Сучасні технології дозволяють створювати автоматичні системи для поширення пропаганди. Такі системи включають:

– соцмережевих ботів, які автоматично генерують пости та коментарі;

– фарм акаунтів, що створюють видимість підтримки певних ідей;

– автоматизовані генератори фейкових новин, що застосовують алгоритми для швидкого створення та розповсюдження контенту [8].

Приклад: Під час Brexit зафіксовано численні випадки використання ботів для поширення маніпулятивної інформації на користь виходу Великої Британії з ЄС.

Застосування спільних платформ для інтеграції військових, економічних та політичних стратегій дає змогу посилювати вплив. Цифрові платформи забезпечують координацію дій, зокрема:

– аналіз даних про цільову аудиторію;

– контроль за поширенням інформації;

– розподіл ресурсів для проведення кампаній.

Китай застосовує інтегровані комунікаційні платформи для координації своїх ініціатив, таких як «Один пояс, один шлях». Це дає змогу синхронізувати дії на державному, економічному та інформаційному рівнях.

У табл. 6 розглянемо технології інтеграції впливу [9].

Поєднання кібероперацій, автоматизації пропаганди, аналізу великих даних та використання ШІ створює умови для одночасного впливу на різні аспекти життя суспільства. Це робить такі операції більш ефективними, але також підвищує необхідність посилення заходів з протидії, розроблення національних стратегій інформаційної безпеки та інноваційних рішень для захисту від комплексних загроз.

Діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері є важливим елементом сучасних загроз для національної безпеки. Ці структури застосовують інформаційні операції для досягнення стратегічних цілей, впливу на політичну ситуацію, економіку та внутрішню стабільність країн [10]. У відповідь на ці загрози держави повинні розробляти ефективні механізми захисту та забезпечення інформаційної безпеки, а також посилювати міжнародне співробітництво для протидії зовнішнім інформаційним впливам.

Таблиця 6 – **Технології інтеграції впливу**

Технологія	Функція	Приклад застосування
Координація кібероперацій	Організація атак на інфраструктуру разом із поширенням дезінформації	Атака на інфраструктуру України (2015 р.) із синхронною пропагандою
Штучний інтелект	Аналіз даних, створення персоналізованих інформаційних атак	Cambridge Analytica під час виборів у США (2016 р.)
Автоматизація пропаганди	Використання ботів і алгоритмів для поширення фейкових новин	Бот-мережі під час Brexit
Інтеграція комунікацій	Використання платформ для координації політичних, економічних і військових дій	Китайська ініціатива «Один пояс, один шлях»

Список використаних джерел

1. Координація розвідувальної діяльності: досвід інших країн: аналітичний матеріал. *Національний інститут стратегічних досліджень*. URL: https://niss.gov.ua/sites/default/files/2020-04/rozvid-diyalnist-dosvid-inshyh-krain-2.pdf
2. Основи розвідувальної діяльності. URL: https://bintel.org.ua/nukma/rozviduvalna_dijalnist/
3. Поняття OSINT та суміжні категорії: наукове дослідження. *Львівський національний університет імені Івана Франка.* URL: https://www.lsej.org.ua/9_2024/80.pdf
4. Правові засади організації та функціонування розвідки: наукова стаття. *Практика державного управління*. URL: https://pgp-journal.kiev.ua/archive/2021/2/21.pdf
5. Про розвідку: Закон України від 17 вересня 2020 року № 912-20. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/go/912-20
6. Розвідка на основі відкритих джерел. *Вікіпедія.* URL: https://uk.wikipedia.org/wiki/Розвідка_на_основі_відкритих_джерел
7. Розвідка на основі відкритих джерел. *Львівська політехніка*. URL:https://lpnu.ua/sites/default/files/2021/pages/12564/rozvidka.pdf
8. Роль інформаційного простору у забезпеченні національної безпеки: наукова стаття. *Academy Vision*. URL: https://academy-vision.org/index.php/av/article/download/605/553/558
9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021. *Офіційний сайт Президента України*. URL: https://www.president.gov.ua/documents/6852021-41069
10. Козубцов І.М., Ткач В.О., Глобін А.В., Фомкін Д.В. Уповноваження органів сектору безпеки та оборони. *Наука і техніка.* 2021. URL: https://lib.iitta.gov.ua/id/eprint/736511/

References

1. Coordination of Intelligence Activities: Experience of Other Countries: Analytical Material. *National Institute for Strategic Studies*. URL: https://niss.gov.ua/sites/default/files/2020-04/rozvid-diyalnist-dosvid-inshyh-krain-2.pdf (in Ukrainian).
2. Basics of Intelligence Activities. URL: https://bintel.org.ua/nukma/rozviduvalna_dijalnist/ (in Ukrainian).
3. The Concept of OSINT and Related Categories: Scientific Research. *Ivan Franko National University of Lviv*. URL: https://www.lsej.org.ua/9_2024/80.pdf (in Ukrainian)
4. Legal Foundations of Organization and Functioning of Intelligence: Scientific Article. *Public Administration Practice*. URL: https://pgp-journal.kiev.ua/archive/2021/2/21.pdf (in Ukrainian).
5. On Intelligence: Law of Ukraine dated September 17, 2020, No. 912-20. *Bulletin of Verkhovna Rada of Ukraine*. URL: https://zakon.rada.gov.ua/go/912-20 (in Ukrainian).
6. Open-Source Intelligence (OSINT). *Wikipedia*. URL: https://en.wikipedia.org/wiki/Open-source_intelligence (in Ukrainian).
7. Open-Source Intelligence. *Lviv Polytechnic National University*. URL: https://lpnu.ua/sites/default/files/2021/pages/12564/rozvidka.pdf (in Ukrainian).
8. The Role of the Information Space in Ensuring National Security: Scientific Article. Academy Vision. URL: https://academy-vision.org/index.php/av/article/download/605/553/558 (in Ukrainian).
9. Presidential Decree of Ukraine No. 685/2021. Official Website of the President of Ukraine. URL: https://www.president.gov.ua/documents/6852021-41069 (in Ukrainian).
10. Kozubtsov I.M., Tkach V.O., Hlobin A.V., Fomkin D.V. Empowerment of Security and Defense Sector Bodies. *Science and Technology*. 2021. URL: https://lib.iitta.gov.ua/id/eprint/736511/ (in Ukrainian).

Mykhailo SHEVCHUK
PhD in Legal Sciences, doctoral student, Leonid Yuzkov Khmelnytskyi University of Management and Law
ORCID: https://orcid.org/0000-0001-7549-6344
e-mail: m.shevchuk522@gmail.com

ANALYSIS OF EXTERNAL SOURCES OF STATE INFORMATION DANGER

This paper examines external sources of information threats to state security, focusing on the activities of foreign political, military, economic, and intelligence structures in the information sphere. It analyzes the implications of global dominance policies in information domains, the role of international terrorist organizations, and the development of concepts for information warfare. Additionally, the paper highlights cultural expansion strategies targeted at specific nations and explores integrated approaches that combine technology and information manipulation to amplify influence. Key attention is given to modern methods employed in cyber-espionage and their impact on national security frameworks. It emphasizes the economic ramifications of information manipulation, including market destabilization and unfair competitive advantages driven by disinformation campaigns. Furthermore, the study explores the increasing reliance on artificial intelligence and machine learning tools for both defensive and offensive purposes in the information space. Special attention is given to collaborative international efforts to counteract these threats and the need for unified global policies to ensure information sovereignty and security. The study underscores the importance of fostering international cooperation, enhancing cybersecurity infrastructure, and promoting public awareness to combat the challenges posed by foreign interference and information warfare. By bridging theoretical perspectives with practical applications, this paper serves as a valuable resource for policymakers, security analysts, and researchers dedicated to safeguarding national interests in an increasingly interconnected and vulnerable information environment. The research contributes to a deeper understanding of how integrated technological and informational tools are used to influence state stability and highlights the urgent need for adaptive and proactive measures in the digital age. The study is grounded in recent scientific works and practical insights, providing a comprehensive overview of unresolved issues and suggesting areas for further research.

Keywords: *external sources, information security, disinformation, cyber threats, political influence, international terrorist groups, information wars, cultural expansion, intelligence structures, information operations, dominance in the information sphere, geopolitical threats, defense strategies*