Valerii Borokhvostov, Lesia Skurinevska, Julia Lutsik (2019) Informatsiyno-finansovi tekhnolohiyi hibrydnoyi viyny: metodolohichni pidkhody do analizu zmistu, vynyknennya, reahuvannya ta zapobihannya, [Information and financial technologies of hybrid wars: methodological approaches to the analysis of the content, occurrence, response and prevention]. *Social development & Security*. 9(6), 56 – 76. DOI: <http://doi.org/10.33445/sds.2019.9.6.5>

Інформаційно-фінансові технології гібридної війни: методологічні підходи до аналізу змісту, виникнення, реагування та запобігання

Валерій Борохвостов *, Леся Скуріневська **, Юлія Луцик ***

* Центральний науково-дослідний інститут Збройних Сил України, проспект Повітрофлотський, 28, м. Київ-049, 03049, Україна, e-mail: bvk51@ukr.net, к.т.н. доцент, провідний науковий співробітник.

** Національний університет оборони України імені Івана Черняхівського, проспект Повітрофлотський, 28, м. Київ-049, 03049, Україна, e-mail: olesya201405@gmail.com, к.військ.н., доцент кафедри економіки та фінансового забезпечення.

*** Національний університет оборони України імені Івана Черняхівського, проспект Повітрофлотський, 28, м. Київ-049, 03049, Україна, e-mail: julia.lutsik@gmail.com, к.економ.н., начальник кафедри економіки та фінансового забезпечення.

Article history:

Received: November 10, 2019
1st Revision: December 10, 2019
Accepted: December 30, 2019

Анотація: У статті розглянуті цілі й способи застосування інформаційно-фінансових технологій у так званих гібридних війнах, які стали активно застосовуватися багатьма впливовими країнами світу останнім часом. Для їх своєчасного виявлення, аналізу, розробки способів реагування на них та їх запобігання авторами запропоновані науково-методичний апарат та відповідні методики. Автори роботи

звертають увагу на те, що останнім часом у світі все частіше переходять від традиційних способів ведення війн до новітніх, менш витратних в економічному плані. Одним з таких видів війн є так звані гібридні війни. Цей вид війн має багато аспектів, але автори даної статті зупинилися тільки на одному з них, інтерес до якого виник останнім часом, а саме – на інформаційно-фінансових технологіях (ІФТ) ведення даного типу війн. Виходячи з цього, у статті розкритий зміст ІФТ гібридних війн та основні цілі, які при цьому переслідує так звана «країна – агресор», та наведена розроблена її авторами загальна схема науково-методичного апарату проведення досліджень проявів ІФТ гібридної війни, який складається з етапу встановлення фактів виникнення проявів ІФТ гібридної війни та трьох взаємопов'язаних методик: методики аналізу проявів ІФТ гібридної війни; методики розробки способів реагування на прояви ІФТ гібридної війни; методики розробки та втілення заходів щодо запобігання підстав для виникнення проявів ІФТ гібридної війни тощо. У подальшому

матеріалі статті викладені схеми та докладний зміст означених методик. Автори статті наголошують на тому, що для протидії проявам ІФТ гібридної війни має здійснюватися розробка заходів, спрямованих на усунення наслідків установлених негативних фактів, а також на запобігання виникнення у майбутньому у «країні – мішені» випадків, які призводять, або можуть призвести до їх появи. Задля цього вони пропонують спеціально призначену для цього методику, схема та загальний зміст якої також наведені у статті. Головне, на чому вони наполягають, це те, що у країні не повинні створюватися підстави для звинувачення її або її керівників у фінансових махінаціях. Й що тільки так можна буде запобігати застосування по відношенню до неї ІФТ гібридної війни.

Ключові слова: гібридна війна, інформаційна компанія, інформаційно-фінансові технології, «країна – агресор», «країна – мішень», фінансовий скандал.

Бібл.2, мал. 7.

1. Постановка проблеми

1.1. Новизна дослідження.

Стаття є результатом аналізу, узагальнення та подальшого опрацювання окремих досліджень у сфері **інформаційно-фінансових технологій (ІФТ)** гібридної війни, зокрема [1, 2]. Автори статті використали з цих матеріалів окремі положення для ілюстрації розробленого ними науково-методичного апарату, а також для побудови схем, наведених на мал. 1 та 2. Запропоновані у статті методичний апарат, методики та всі інші схеми (мал.3 – 7) є оригінальними та є результатом аналітичної діяльності й особистої думки авторів роботи.

1.2. Аналіз останніх досліджень та публікацій

Останнім часом у світі поширюються думки про те, що, крім звичайних способів збройної боротьби, передові країни світу все частіше застосовують й ведуть так звані **гібридні війни**. Тому, проблематика гібридної війни все частіше привертає до себе увагу аналітиків й спеціалістів (й не тільки військових) багатьох країн світу. У той же час, погляди аналітиків у цій сфері різних країн декілька різняться поміж собою [1, 2].

Технології гібридної війни

Зокрема, у США концепцію гібридної війни одним з перших розпочав розробляти колишній морський офіцер Франк Хофман. За його дослідженнями, тактику гібридної війни уперше застосувала Хезболла у 2006 році під час палестино-ізраїльського конфлікту. Виходячи з аналізу його змісту, Франк Хофман надав розгорнуту характеристику гібридної війни, яку він назвав «війною майбутнього», «конфліктом ХХІ століття». Він зазначив, що гібридні війни – набагато більше, ніж прості конфлікти між державами та іншими збройними групами. Це – застосування різних форм конфліктів, які краще позначити як гібридні загрози або конфлікти, які можуть вестися як державами, так й різними недержавними суб'єктами, які, як правило, спрямовуються й координуються оперативно і тактично всередині основного поля бою для

досягнення синергетичного ефекту фізичних і психологічних аспектів конфлікту.

Декілька пізніше гібридні війни, їх зміст та особливості почали досліджувати у Російській Федерації (РФ). Зокрема, начальник Генерального штабу Збройних Сил (ЗС) РФ Валерій Герасимов у 2013 році зазначив, що у XXI столітті простежується тенденція стирання різниці між станом війни та миру. Війни вже не оголошуються, а розпочавшись – йдуть за незвичним для більшості осіб, що беруть у них участь та досліджують проблеми війни і миру, шаблоном. Він також відмітив, що у сучасних конфліктах, які виникають поміж окремими державами, акцент форм вирішення міждержавних конфліктів та методів, що при цьому використовуються, усе більше зміщується у бік комплексного застосування політичних, економічних, інформаційних та інших заходів невоєнного характеру, які практично завжди реалізуються зі спиранням на воєнну силу (мал. 1).

Мал. 1 – Технології гібридної війни

Дані методи він називає гібридними. Їх зміст полягає у досягненні політичних цілей, яка ставить перед собою та або інша держава, з мінімальним застосуванням на противника воєнних засобів. Перевага над противником при цьому досягається за рахунок підриву його воєнного і економічного потенціалу, інформаційно-психологічного тиску, активної підтримки внутрішньої опозиції, партизанських та диверсійних методів тощо.

У зв'язку з тим, що тема гібридної війни у даній статті не ставиться за мету докладного розглядання, ми зосередимося тільки на одному з її аспектів, інтерес до якого виник останнім часом, а саме – на **інформаційно-фінансових технологіях** [1], які стали широко застосовуватися різними державами. Зміщення акценту з прямих воєнних дій та воєнних інтервенцій до гібридних методів впливу на противника, на думку воєнних дослідників, є набагато менш

витратним, у той же час – надзвичайно ефективним як з воєнної, так і з економічної точки зору.

Цілі та основні способи застосування ІФТ гібридної війни

Дослідники у сфері ІФТ гібридної війни зазначають, що під час їх застосування на перший план висувається *тенденційно підібрана інформація щодо негативних явищ у фінансових процесах країни*, на яку хочуть зробити вплив (будемо називати її «країною – мішенню») з боку країни, яка ставить за мету підкорити цю країну своїм економічним та фінансовим інтересам (назвемо її «країною – агресором»), яка багатократно підсилюється підконтрольними цій країні (або її визначеним колам) засобами масової інформації (ЗМІ), а також, часто, ЗМІ країн, які залежать від цієї «країни – агресора» політично й економічно.

Основні цілі ІФТ гібридної війни з боку «країни – агресора» містяться у лівій частині схеми, зображеної на мал. 2 [1].

Мал. 2 – Цілі та основні способи застосування інформаційно-фінансових технологій гібридної війни

Зазначені цілі наведені, починаючи з менших з них (цілі «а» – «в»), які, так би мовити, є цілями залякування керівництва та населення «країни – мішені», і закінчуючи найбільш радикальними (цілі «г» – «з»), якщо втіленням попередніх цілей не вдасться досягнути головної мети даної гібридної війни, яка полягає у повному або у близького до повного економічному та політичному

підпорядкуванні (звичайно, замаскованого) «країни – мішені» «країні – агресору». При цьому, ІФТ у вигляді податкових, корупційних або інших фінансових скандалів за більшістю випадків є інформаційним поводом для стимулювання масових виступів населення проти урядів й дуже часто приводить до зміни режиму у «країні – мішені».

У доповнення до цих узагальнених цілей кожний конкретний приклад застосування ІФТ гібридної війни має свої специфічні завдання. При чому, в окремих випадках використовуються широкомасштабні та багатоцільові технології, іноді замасковані під «благі наміри» з боку «країни – агресора», які одночасно можуть уражати багато країн та компрометувати їх лідерів.

Досягнення наведених цілей ІФТ гібридної війни, на думку дослідників, можливе *трьома основними способами*, що містяться у правій частині схеми на мал. 2, кожний з яких може застосовуватися як окремо, так і, при масовому «наступі» – усі разом, або у будь-якій іншій комбінації [1].

До цього слід додати, що зараз поле боротьби з фінансовими злочинами, зокрема з корупцією, іноді розширюється до абсурду. Під реальне або надумане звинувачення у корупції тепер можна підвести ще й звинувачення у сприянні тероризму. Логіка приблизно така: якщо «м'які» ненасильницькі антикорупційні демонстрації не приведуть до бажаного «країні – агресору» результату і «диктатор» у «країні – мішені» усидить на своєму троні, наступним етапом буде звинувачення його у сприянні тероризму, що в очах широкої світової спільноти послужить вагомим виправданням воєнної інтервенції.

1.3. Постановка завдання

У той же час слід зазначити, що зміщення акценту з прямих воєнних інтервенцій до гібридних методів ведення війни призведе до все більшого застосування ІФТ гібридної війни, у тому числі – антикорупційних сценаріїв, які є мало витратними, проте надзвичайно ефективними. Це пов'язано із тим, що корупція та інші фінансові зловживання як такі не привносяться ззовні, вони вже існують всередині державного організму. Задача гібридного противника («країни – агресора») полягає у тому, щоб за допомогою медійних кампаній соціальних мереж та ЗМІ зробити факти корупції відомими для широкої спільноти, спровокувати масові безпорядки, стимулювати створення опозиційних антикорупційних рухів і організацій, ініціювати політизовані судові процеси тощо. Саме вивчення цих процесів та розробка дійових механізмів щодо їх запобігання й ставиться за *метою даної статті*.

2. Виклад основного матеріалу

Загальна схема науково-методичного апарату проведення досліджень проявів ІФТ гібридної війни

Відносно слабкі у воєнному, економічному та політичному плані країни, до яких відносяться невеликі країни, і до яких певною мірою можна віднести й Україну, не можуть застосовувати весь спектр ІФТ гібридної війни проти своїх дійсних та ймовірних противників. У той же час, вони часто мають

«оборонятися» від таких нападів або заяв (звинувачень) з боку деяких інших країн, потужних у воєнному та економічному плані, і які мають відносно даної країни (або навколо неї) свої національні інтереси. Для ефективної «оборони» від цих країн, а також для наведення порядку у фінансовій сфері власної країни, на нашу думку, потрібні певні технології. Знайти їх, у деякій мірі, можливо за допомогою **науково-методичного апарату (НМА) та методик**, схеми та загальний зміст яких пропонуються у даній роботі.

Загальна схема НМА проведення досліджень проявів ІФТ гібридної війни, що пропонується у даному дослідженні, наведена на мал. 3.

Мал. 3 – Загальна схема науково-методичного апарату проведення досліджень проявів інформаційно-фінансових технологій гібридної війни

Даний НМА складається з етапу встановлення фактів виникнення проявів ІФТ гібридної війни та трьох взаємопов'язаних методик:

методики аналізу проявів ІФТ гібридної війни;

методики розробки способів реагування на прояви ІФТ гібридної війни;

методики розробки та втілення заходів щодо запобігання підстав для виникнення проявів ІФТ гібридної війни тощо.

Загальна схема встановлення фактів виникнення проявів ІФТ гібридної війни

На даному етапі дослідження встановлюються, констатуються та попередньо аналізуються наявні факти застосування проти «країни – мішені» яких-небудь проявів ІФТ та інших методів гібридної війни.

Дослідники у цій сфері зазначають, що признаками застосування ІФТ можуть бути [1]:

1) одночасне з'явлення у ЗМІ та у виступах окремих осіб інформації з компрометом, яка супроводжується тенденційними коментарями аналітиків та дослідницьких інститутів;

2) джерелом негативної інформації, проміж інших, є фонди у «країні – мішені», що фінансуються іноземними країнами, та які отримують інформацію щодо «своїх» країн від різних інформаторів або анонімних осіб, та завдання щодо її оприлюднення;

3) включення «країни – мішені» до числа загроз національній безпеці будь-яким іншим країнам, які й до цього часу здійснювали ворожу (явну або приховану) політику по відношенню до «країни – мішені», або мали до неї будь-які претензії (зазіхання) в політичній, економічній, фінансовій та інших сферах, та включення положень щодо цього у свої доктринальні документи;

4) заяви лідерів окремих впливових країн світу щодо необхідності «демократичних» реформ у «країні – мішені»;

5) активізація дій у «країні – мішені» організацій, агресивних та опозиційних по відношенню до діючої влади, спрямованих на влаштування масових безпорядків й заворушень, та отримання, на цій основі різних дивідендів для себе (наприклад, завоювання влади, або отримання впливових посад при діючій владі);

6) інформаційна компанія у ряді країн, в якій чинні керівники «країни – мішені» оголошуються джерелами загроз не тільки для власної держави, а й загрозами для усього останнього «демократичного» світу;

7) одночасне із зазначеними, використання інших інструментів гібридної війни тощо.

При встановленні фактів застосування проти «країни – мішені» проявів ІФТ гібридної війни доцільно розглянути ряд специфічних питань (мал. 4), які слугуватимуть підґрунтям для подальшого більш глибокого аналізу події, що сталися, та розробці методів й способів офіційної реакції за його результатами.

На думку авторів даної роботи, на цьому етапі доцільно розглянути й проаналізувати такі питання:

час виникнення проявів ІФТ гібридної війни;

країни оприлюднення проявів ІФТ гібридної війни;

джерела та способи оприлюднення проявів ІФТ гібридної війни;

зміст (сутність) проявів ІФТ гібридної війни (відповідно до мал. 1).

За необхідності, перелік питань, що розглядаються, може бути змінений або розширений, залежно від сутності, видів та способів конкретних проявів ІФТ гібридної війни, що застосовуються у кожному конкретному випадку.

В якості прикладу встановлення фактів виникнення проявів ІФТ гібридної війни можна навести опубліковані в одному з аналітичних досліджень події 2013-2016 рр., коли відбулося кілька крупних вкидань компромату, які одночасно опублікували близько 40 провідних світових видань, таких як BBC Panorama, EL Pais (Іспанія), L'espresso (Італія), Le Monde (Франція), Новая газета (Росія), Sueddeutsche Zeitung (Німеччина), The Guardian (Великобританія), The New York Times (США), The Washington Post (США) тощо [1].

Мал. 4 – Загальна схема встановлення фактів виникнення проявів інформаційно-фінансових технологій гібридної війни

Ця широкомасштабна компанія була ініційована так званим Міжнародним консорціумом журналістських розслідувань (далі – Консорціум або ICIJ), створеним у Вашингтоні у 1997 році американською некомерційною організацією «Центр за чесність у суспільстві» (Center for Public Integrity), до складу якого входять 160 відомих журналістів із різних країн. Інформаційна бомба вибухнула у квітні 2013 року, коли ICIJ, та провідні світові видання, асоційовані із ICIJ, одночасно опублікували на перших сторінках сенсаційні повідомлення щодо зв'язків відомих політичних діячів та світових знаменитостей з офшорними компаніями. У доповіді під назвою «Offshore Leaks» були розкриті дані щодо 130 тис. рахунків в офшорних банках. При цьому дослідження ґрунтувалося на контент-аналізі 2,5 млн. таємних файлів щодо активів фізичних осіб із 170 країн, які були виведені у офшори.

У доповіді ICIJ були зроблені висновки, які відносяться до такого:

- урядові чиновники Китаю, Азербайджану, Росії, Канади, Пакистану, Філіппін, Таїланду, Монголії та багатьох інших країн, а також їх родичі й наближені особи використовували анонімні компанії та банківські рахунки, нелегальні схеми, які недоступні для звичайних громадян;
- багато з великих банків світу, у тому числі UBS, Credit Suisse и Deutsche Bank, активно спрямовували своїх клієнтів у офшорні сховища на Британських Віргінських островах та ін.;

- ціла індустрія добре оплачуваних бухгалтерів, посередників і консультантів допомагали офшорним власникам приховувати свою ідентичність та бізнес-інтереси, покриваючи у багатьох випадках відмивання грошей та інші неправомірні дії;

- фінансові махінатори та інші крупні шахраї звичайно використовують офшорні зони для того, щоб приховати гроші, які отримані нечесним шляхом, а також щоб уникнути підвищеного оподаткування у власних країнах тощо.

Іншим аналогічним та найбільш потужним офшорним скандалом стала публікація ICIJ у квітні 2016 року так званого «Панамського дос'є» щодо діяльності й клієнтів маловідомої панамської юридичної фірми Mossack Fonseca [1]. З квітня 2016 року ICIJ та деякі інші впливові західні ЗМІ стали публікувати статті, що ґрунтувалися на 11,5 млн. документів, «здобутих» із бази даних цієї фірми, які демонстрували приховані багатства політиків, знаменитостей та інших осіб.

«Панамські документи» охоплювали період майже у 40 років: з 1977 до грудня 2015 року. Вони містили докладну інформацію щодо 200 тис. непрозорих офшорних компаній, трастів та фондів, що використовувалися клієнтами Mossack Fonseca. У центрі уваги також опинилися заморські території Великобританії, які є важливими гвинтиками в офшорному механізмі. Про це свідчить хоча б те, що із 200 тис. компаній, які згадані у «Панамському дос'є», половина зареєстрована на Британських Віргінських островах.

Наведені два приклади фінансових скандалів стосуються багатьох країн світу (за деякими виключеннями). У той же час, аналіз світових ЗМІ свідчить, що у багатьох випадках та публікаціях об'єктами критики є не офшорні компанії як такі, а окремі особи – олігархи, політики та урядові чиновники, або окремі «країни – мішені». Також іноді згадуються всесвітньо відомі банки, транснаціональні корпорації та фінансові групи тощо.

Саме на цей момент й доцільно звернути найбільш щільну увагу під час встановлення та аналізу проявів застосування ІФТ гібридної війни проти конкретної «країни – мішені» та її окремих діячів.

Схема та загальний зміст методики аналізу проявів ІФТ гібридної війни

Запропоновані НМА та порядок встановлення фактів виникнення проявів ІФТ гібридної війни надали можливість побудувати методику їх аналізу, загальна схема якої представлена на мал. 5.

Дана методика складається з чотирьох взаємопов'язаних блоків:

1 блок. Аналіз змісту (сутності) проявів ІФТ гібридної війни.

2 блок. Аналіз часу виникнення проявів ІФТ гібридної війни.

3 блок. Аналіз країни (країн) оприлюднення проявів ІФТ гібридної війни.

4 блок. Аналіз джерел оприлюднення проявів ІФТ гібридної війни.

Аналіз змісту (сутності) проявів ІФТ гібридної війни передбачає проведення досліджень, у ході яких необхідно з'ясувати ряд питань, головними з яких є:

- на що або на кого спрямовані звинувачення (країна у цілому або її окремі політичні діячі (сили);

Мал. 5 – Загальна схема методики аналізу проявів інформаційно-фінансових технологій гібридній війні

- який спосіб (відповідно до мал. 1) ІФТ гібридної війни застосовано та його сутність.

У наслідок їх ретельного опрацювання має бути зроблено первинне з'ясування щодо правомірності висунутих звинувачень та застосування ІФТ гібридної війни.

Більш глибокий аналіз гучних фінансових скандалів у світі показує, як здійснюється еволюція від засобу боротьби з офшорами, який має позитивну ціль – скоротити ухиляння від сплати податків у власних країнах, до перетворення їх у багатоцільову зброю гібридної війни, спрямовану на дискредитацію керівників країн, які опираються політиці домінування «країни – агресора». Зокрема, публікація «Панамського дос'є», на думку дослідників, що переймалися даним питанням, мала з боку «країни (країн) – агресора» широкий спектр геофінансових та геополітичних цілей, у тому числі [1]:

Ціль 1 – дискредитація лідерів країн, які проводять або намагаються проводити незалежну від «країни – агресора» політику.

Огляд світових ЗМІ з даного питання свідчить, що у багатьох публікаціях основна увага та основний «напрямок удару» спрямований не на офшори, як первопричину фінансових зловживань, а на окремих «гравців», які знаходяться у владі у «країнах – мішенях». У той же час, проведені дослідження [1] свідчать, що більша частина незаконних фінансових потоків та зловживань у фінансовій сфері (близько 60-65 %) є результатом комерційної діяльності, в основному, у формі маніпуляцій з рахунками-фактурами та інших форм ухиляння від сплати податків. Ще 30-35% є результатом чисто кримінальної діяльності. У той же час, корупція з боку впливових політичних гравців різних країн, яку часто вважають головною причиною фінансових втрат, становить лише близько 3 %.

Ціль 2 – політичний шантаж.

ІФТ гібридної війни, у більшості випадків, є засобом натякання окремим лідерам країн, політичним діячам, визначеному колу впливових у своїх країнах осіб та фірм про те, що у «країні – агресорі» щодо них є велика кількість компромату, який буде опублікований у випадку їх непокори, якщо дана особа (особи) не будуть виконувати «завдання», які ставляться або будуть ставитися перед ними. Шляхом такого шантажу дана особа (особи) будуть постійно знаходитися на «гачку» й виконувати всі завдання, які їм будуть ставитися, іноді навіть на шкоду власній країні.

Ціль 3 – спрямування фінансових потоків із розгромлених офшорів у більш грошові та респектабельні (наприклад, британські та американські) податкові «гавані».

Багато хто з дослідників вважають, що «країни – агресори», які розпочинають масові інформаційно-фінансові скандали, намагаються при цьому знищити конкурентів у цій прибутковій нелегальній сфері діяльності.

Зокрема, Панамський скандал має безсумнівні ознаки ІФТ мережецентричної гібридної війни: різнорідна група недержавних суб'єктів, які начебто діють без централізованого керівництва, здійснює інформаційну атаку, яка не випадково співпадає з міжнародними політичними цілями окремих

впливових країн. На думку про це наштовхує те, що у даному скандалі практично немає звинувачень у бік представників цих країн.

Тому, аналізуючи будь-який скандал, який має ознаки ІФТ гібридної війни, необхідно обов'язково проаналізувати питання: кому (якій країні, або фінансовим колам якої країни) є вигідним проведення подібної операції, та якою може бути реакція «країни (країн) – мішені».

Скандали, подібні Панамському, служать попередженням тим, хто бажає брати участь в офшорному бізнесі та бажає уникнути витоку небажаних відомостей про це або юридичних розслідувань. Тобто, дана особа (особи), якщо вона (вони) не хочуть мати неприємностей, повинні місцем приховування своїх цінностей обрати саме надійно захищені всіма можливими способами сховища у визначеній країні (якою, як правило, є «країна – агресор», яка старанно приховує свою причетність до створення цього скандалу).

Ціль 4 – війна із збереженнями та перехід до безготівкового суспільства.

Окремі міжнародні спеціалісти у фінансовій сфері висловлюють думку про те, що скандали, подібні Панамському, є частиною війни, що поступово розгортається, за контроль над капіталом, який безпосередньо пов'язаний із переходом до біометричної цифрової валюти, застосуванням відніманих процентних ставок, багато масштабних системних порятунків банків у формі bail-in (примусова конвертація незабезпечених вимог кредиторів третьої черги у субординовані депозити або уставний капітал банку), демонізацією та можливою криміналізацією фізичних активів, що знаходяться за межами прямого контролю податкових органів тощо. На їх думку, зроблено це буде під вивіскою боротьби з «податковими сховищами», й основними мішенями при цьому будуть готівкові гроші та дорогоцінні метали.

Ціль 5 – (ретельно замаскована) – отримання й накопичення інформації щодо руху активів по усьому світові під прикриттям боротьби за фінансову прозорість.

Зокрема, оприлюднення «Панамських документів» стимулювало бурну діяльність різних міжнародних організацій, національних фінансових та податкових відомств із реформування міжнародного податкового законодавства.

Аналіз часу виникнення проявів ІФТ гібридної війни передбачає проведення досліджень, у ході яких з'ясовується: які події у політичному житті «країни – мішені», або у поведінку окремих політичних діячів (сил) передували оприлюдненню проявів проти неї (них) ІФТ гібридної війни, або які мають відбутися, та які могли спровокувати їх з'явлення.

Зокрема, якщо є намагання не допустити до влади якогось політичного діяча, небажаного з точки зору виконання «завдань» на користь «країни – агресора», то компромат на нього публікується перед черговими виборами до органів влади у «країні – мішені». Це ж саме робиться й під час бажання політичного діяча балотуватися на посаду на другий та інші терміни. Причому, обсяги даного компромату та інформація, що у ньому міститься, у даних випадках повністю компрометують дану особу як в очах населення країни, так й в очах світового суспільства. Якщо в даній країні панує верховенство права та законів, то шлях для такого діяча до бажаної влади може бути зачинений.

У такий же спосіб застосовуються ІФТ по відношенню до керівництва країн або їх окремих впливових політичних діячів, якщо вони насправді скомпрометували себе перед світовою спільнотою, та «країна – агресор» вже не може їх підтримувати за міркуваннями підтримки свого міжнародного іміджу як прихильника та ярого борця за демократію в усьому світі, або вони перестали «прислуховуватися» до порад і рекомендацій своїх «кураторів» з «країни – агресора».

У випадку, якщо компромат публікується після виборів або у дозований спосіб (тільки деякі окремі дані, які за бажанням можна буде якось спростувати або обійти замовчуванням), то це може свідчити про те, що керівництво «країни – агресора» натякає таким особам про те, що у них є ще більш вагомні «аргументи», які можуть їм суттєво нашкодити або навіть знищити їх політичну кар'єру, якщо вони не будуть «слухняними» й не будуть у своїй подальшій діяльності дотримуватися, як й у попередньому випадку, рекомендацій своїх «кураторів» з «країни – агресора».

Аналіз країни (країн) оприлюднення проявів ІФТ гібридної війни передбачає проведення досліджень, у ході яких з'ясовуються:

стан стосунків «країни – мішені» з «країнами – агресорами», які застосували проти неї дані ІФТ гібридної війни;

які дії «країни – мішені» або її окремих політичних діячів (сил) могли спровокувати «країни – агресори» застосувати проти неї дані ІФТ гібридної війни тощо.

При цьому, як слідує з мал. 4, «країни – агресори» по відношенню до «країни – мішені» у попередніх стосунках могли бути або дружніми («країни – друзі»), або недружніми («країни – вороги» або «країни – суперники»).

Те, що елементи ІФТ гібридної війни проти «країни – мішені» застосовують «країни – вороги» або «країни – суперники», які увесь час до того намагалися впливати на дану країну в ідеологічній, економічній, політичній, соціальній та інших сферах життя, не викликає особливих здивувань. До «нападу» з цього боку у «країни – мішені» готовляться завжди (але, як показує практика, не завжди повністю готові, тому що супротивник майже завжди знаходить «слабкі місця» у «країни – мішені»).

Інша справа, коли ІФТ, які можна розцінювати як елементи або прояви гібридної війни, застосовують країни, які до цього моменту були, або принаймні вважалися дружніми по відношенню до «країни – мішені». У цьому випадку слід ретельно проаналізувати: що до цього привело, й досягнення яких цілей ставлять перед собою дані «країни – друзі». Частково відповіді щодо цих питань були розкриті під час розглядання перших двох етапів даного аналізу. У той же час, слід розуміти, що керівництво кожної країни основні свої зусилля як у внутрішній, так й особливо у зовнішній політиці спрямовує на захист національних інтересів, економічне процвітання й добробут власної країни, й намагається підкорити даним інтересам не тільки своїх «ворогів», але й, у першу чергу (це досягти простіше), своїх так званих «друзів». Тому на практиці може статися так, що той, хто на словах видавав себе за друга, насправді є, у кращому

випадку, байдужим до національних інтересів інших країн, а у гіршому випадку – у будь-який момент може стати для неї ворогом (вовк у ягнячій шкурі).

Одночасно із наведеними вище, здійснюється **аналіз джерел оприлюднення проявів ІФТ гібридної війни**, який буде на користь у справі встановлення причини та справжньої суті висунутих проти «країни – мішені» звинувачень.

Насамперед, аналізується, у який спосіб, зазначений на мал. 4, була оприлюднена негативна для «країни – мішені» інформація. Далі, на нашу думку, потрібно з'ясувати:

кому підпорядковані (ким контролюються) ЗМІ, які оприлюднили негативну інформацію, що містить ознаки проявів ІФТ гібридної війни, проти «країни – мішені»;

політичні погляди та відношення до «країни – мішені» впливових політичних діячів «країни – агресора», які застосували проти неї ІФТ гібридної війни.

Аналіз цього питання особливо актуальний, якщо негативна інформація щодо «країни – мішені» з'явилася у ЗМІ країни або країн, які до цього вважалися по відношенню до неї як «країни – друзі».

Одна справа, якщо ЗМІ у цих країнах належать опозиційним до діючої у них влади силам, або політики, які й до цього виступали з негативною інформацією, або також належать до опозиції й негативно відносяться до «країни – мішені» або до її керівництва. Вплив на такі ЗМІ і таких політиків можуть справляти й інші країни, які по відношенню до «країни – мішені» завжди асоціювалися як «країни – вороги».

Інша справа, якщо таку негативну інформацію оприлюднюють ЗМІ або політики, які до цього асоціювалися по відношенню до «країни – мішені» як «країни – друзі». У даному випадку слід провести більш ретельне дослідження – які дії у «країні – мішені», або події у «країнах – друзях» призвели до того, що вони змінили своє ставлення до цієї країни з дружнього до цілком протилежного.

На завершення аналізу усіх зазначених складових здійснюється *узагальнення його результатів та розробляються способи реагування на даний (дані) конкретний прояв ІФТ гібридної війни*.

Схема та загальний зміст методики розробки способів реагування на прояви ІФТ гібридної війни

За результатами проведення всебічного аналізу фактів застосування проти «країни – мішені» ІФТ гібридної війни, розробляються способи й методи реагування на них.

Перш за все, у «країні – мішені» компетентними органами, відповідно до покладених на них повноважень, здійснюється перевірка достовірності оприлюднених фактів за методикою, схема якої зображена на мал. 6.

Результати перевірки можуть бути такими:

- 1) інформація, викладена у звинуваченнях, не підтверджується;
- 2) інформація, викладена у звинуваченнях, підтверджується (повністю або частково).

Мал. 6 – Загальна схема методики розробки способів реагування на прояви інформаційно-фінансових технологій гібридної війни

У першому випадку, якщо дані перевірки є достатньо достовірними, а звинувачені у начебто скоєних ними порушеннях особи впевнені у своїй невинності, то ними, або компетентними органами «країни – мішені», у встановленому національним та міжнародним законодавством порядку, здійснюється подача судового або іншого позову до «країни – агресора» або до окремих її політичних діячів, які оприлюднили недостовірні або скривджені негативні факти відносно «країни – мішені» або окремих її політичних діячів,

щодо притягнення їх до відповідальності відповідно до норм міжнародного права, та зобов'язання їх публічно спростувати свої попередні негативні заяви.

У другому випадку, коли попередня перевірка встановила певну достовірність оприлюднених негативних фактів, компетентними органами «країни – мішені», у встановленому національним законодавством порядку, здійснюється їх поглиблене розслідування із з'ясуванням усіх обставин, які призвели до їх виникнення та оприлюднення «країною – агресором», змісту скоєних правопорушень тощо.

За результатами розслідування відбувається встановлення винних посадових осіб «країни – мішені», ступеню їхньої вини, негативного впливу скоєних ними правопорушень на всі сфери життя та діяльності «країни – мішені», на її міжнародний імідж тощо, а також, якщо це передбачено національним законодавством у цій сфері, – їх покарання.

У даному випадку, на нашу думку, розслідування може відбуватися за кількома сценаріями.

За першим з них, особи, звинувачені у скоєних правопорушеннях, можуть повністю або частково визнати свою провину та доповісти слідству всі обставини цієї справи. У дійсно демократичних країнах (або у країнах, в яких ще якимось дотримуються встановлених демократичних норм і правил) посадові особи, яких звинуватили у фінансових правопорушеннях, якщо вони мають поняття власної гідності, звичайно йдуть зі свого державного поста у відставку (правда, іноді це робиться для того, щоб утримати правосуддя від подальшого розслідування та, у деякому ступеню, приховати від нього всі інші обставини цієї справи). В іншому випадку, якщо із «гідністю» є деякі «компроміси», дані особи добровільно свою посаду не залишають, а чекають на рішення суду, сподіваючись на його більш м'який вирок (якщо буде враховано, що вони самі зізналися та покалися у скоєних ними правопорушеннях).

За другим сценарієм особи, звинувачені у скоєних правопорушеннях, не визнають своєї провини, й усіляко приховують відомості щодо них. Тоді слідству треба буде докласти певних зусиль для з'ясування всіх обставин звинувачень, висунутих «країною – агресором». Зробити це буде достатньо важко, враховуючи те, що розслідування треба буде проводити у міжнародному масштабі, зокрема у країнах, в яких дотримуються (або начебто дотримуються) принципу банківської та іншої фінансової таємниці тощо. Результати такого розслідування багато в чому залежать від «доброї волі» «країни – агресора», представники якої оприлюднили негативні матеріали, зокрема, від того, які цілі публікацією даних матеріалів у даній країні намагаються досягти, та багатьох інших обставин об'єктивного й суб'єктивного характеру.

За третім сценарієм, у «країні – мішені» вся правоохоронна система та система правосуддя можуть бути корумпованими та повністю підпорядкованими (формально або неформально) правлячому режиму, коли на керівних постах органів, що здійснюють дізнання щодо скоєних правопорушень та визначають ступінь відповідальності за них, знаходяться особи, призначені на них із порушенням міжнародних й навіть чинних у даній країні законів і норм (за партійною та політичною приналежністю, родичі, колишні підлегли, особи, які

знаходяться «на гачку» у керівників державної влади тощо). У даному випадку, чекати на справедливий вирок та покарання за скоєний фінансовий злочин не варто. Слідство усіляко буде затягуватися та, у кінцевому результаті, зайде у тупик. З часом усі обставини скандальної справи у суспільстві втратять свою гостроту (будуть забуті або «перекриті» іншими «гучними» справами), а особи, які були звинувачені, й далі будуть продовжувати свою діяльність. При цьому, вони будуть більш ретельно приховувати свої незаконні фінансові оборудки.

Для того, щоб не допускати звинувачень й не доводити до появи випадків застосування проти можливої «країни – мішені» ІФТ гібридної війни, має здійснюватися *розробка заходів, спрямованих на усунення наслідків установлених негативних фактів, а також на запобігання виникнення у майбутньому у «країні – мішені» випадків, які призводять, або можуть призвести до їх появи.*

Загальна схема методики розробки та втілення заходів щодо запобігання підстав для виникнення проявів ІФТ гібридної війни

Розробку та втілення заходів щодо запобігання підстав для виникнення проявів ІФТ гібридної війни пропонується здійснювати за методикою, загальна схема якої представлена на мал. 7.

Головним чинником, необхідним для якісного виконання цієї роботи, є вдосконалення національного законодавства країни, спрямованого на запобігання зловживань всіма посадовими особами держави у фінансовій та інших сферах національної економіки.

Дане вдосконалення має здійснюватися на підставі аналізу національного та передового міжнародного досвіду запобігання та боротьби із зловживаннями у фінансовій сфері, результати якого мають реалізовуватися шляхом розроблення та неухильної реалізації планів, програм, стратегій та інших концептуальних документів, спрямованих на вдосконалення системи запобігання зловживань у цій сфері.

Під час опрацювання, розроблення та реалізації планів заходів щодо запобігання підстав для виникнення проявів ІФТ гібридної війни необхідно використовувати різні способи, спрямовані на безумовне досягнення встановлених цілей, а також керуватися загальноприйнятими у світі принципами, частина з яких наведена на мал. 7.

3. Висновки і перспективи подальших досліджень

Під час роботи над даною статтею її автори не ставили за мету здійснити аналіз і докладне розкриття всіх наведених та інших можливих способів й принципів аналізу, виникнення, реагування та запобігання всіх можливих видів ІФТ. Їх дуже багато. Але, при цьому, на їх думку, має мати місце головне:

Мал. 7 – Загальна схема методики розробки та втілення заходів щодо запобігання підстав для виникнення проявів інформаційно-фінансових технологій гібридної війни

1. Неухильне виконання кожною людиною, особливо держаними посадовими особами, всіх прийнятих у країні законів.

2. Закон має бути єдиним для всіх, незалежно від займаної посади: починаючи від президента країни, й закінчуючи кожною простою людиною.

3. Чим вищу державну посаду займає якась особа, тим більш відповідальною та зразковою в особистому виконанні законів країни та особистому житті вона має бути.

4. Порядку в країні не буде, якщо невиконання чи порушення законів (або їх окремих положень) буде виправдовуватися якою-небудь «доцільністю» (політичною, економічною та іншими). Створений прецедент щодо такого випадку неминуче призведе до систематичних порушень, й, у кінцевому випадку, до руйнування держави.

5. Головним у діяльності кожної посадової особи держави має бути особиста відповідальність за свої дії та неухильне виконання свого призначення: віддана праця на благо своєї країни у цілому й кожного її громадянина окремо.

Саме на дослідження цих питань й розробку практичних рекомендацій з їх виконання й повинні спрямовувати зусилля спеціалістів у сфері державного управління в їх повсякденній діяльності.

Author details (in Russian)

Информационно-финансовые технологии гибридной войны: методологические подходы к анализу содержания, возникновения, реагирования и предотвращения

Валерий Борохвостов *, Леся Скуриневська **, Юлия Луцик ***

** Центральный научно-исследовательский институт Вооружённых Сил Украины, пр-кт Воздухофлотский, 28, г. Киев, 03049, Украина, e-mail: bvk51@ukr.net, кандидат технических наук, доцент, ведущий научный сотрудник.*

*** Национальный университет обороны Украины имени Ивана Черняховського, пр-кт Воздухофлотский, 28, г. Киев, 03049, Украина, e-mail: olesya201405@gmail.com, кандидат военных наук, доцент кафедры экономики и финансового обеспечения.*

**** Национальный университет обороны Украины имени Ивана Черняховського, пр-кт Воздухофлотский, 28, г. Киев, 03049, Украина, e-mail: Julia.Lutsik@gmail.com, кандидат экономических наук, начальник кафедры экономики и финансового обеспечения.*

Аннотация: В статье рассмотрены цели и способы применения информационно-финансовых технологий в так называемых гибридных войнах, которые стали активно применяться многими ведущими странами мира в последнее время. Для их своевременного

выявления, анализа, разработки способов реагирования на них и их предотвращения авторами предложены научно-методический аппарат и соответствующие методики. Авторы работы обращают внимание на то, что в последнее время в мире все чаще переходят от традиционных способов ведения войн к новым, менее затратным в экономическом плане. Одним из таких видов войн являются так называемые гибридные войны. Этот вид войн имеет много аспектов, но авторы данной статьи остановились только на одном из них, интерес к которому возник в последнее время, а именно – на информационно-финансовых технологиях (ИФТ) ведение данного типа войн. Исходя из этого, в статье раскрыто содержание ИФТ гибридных войн и основные цели, которые при этом преследует так называемая «страна - агрессор», и приведена разработанная ее авторами общая схема научно-методического аппарата проведения исследований проявлений ИФТ гибридной войны, который состоит из этапа установления фактов возникновения проявлений ИФТ гибридной войны и трех взаимосвязанных методик: методики анализа проявлений ИФТ гибридной войны; методики разработки способов реагирования на проявления ИФТ гибридной войны; методики разработки и реализации мероприятий по предотвращению оснований для возникновения проявлений ИФТ гибридной войны и тому подобное. В дальнейшем материале статьи изложены схемы и подробное содержание указанных методик. Авторы статьи отмечают, что для противодействия проявлениям ИФТ гибридной войны должны разрабатываться меры, направленные на устранение последствий установленных негативных фактов, а также на предотвращение возникновения в будущем в «стране – мишени» случаев, которые приводят или могут привести к их возникновению. Для этого они предлагают специально предназначенную для этого методику, схема и общее содержание которой приведены в статье. Главное, на что они обращают внимание, это то, что в стране не должны создаваться основания для обвинения ее или ее руководителей в финансовых махинациях. И что только так можно будет предотвращать применение по отношению к ней ИФТ гибридной войны.

Ключевые слова: гибридная война, информационная компания, информационно-финансовые технологии, «страна - агрессор», «страна - мишень», финансовый скандал.

Библ.2, мал. 7.

Author details (in English)

Information and financial technologies of hybrid wars: methodological approaches to the analysis of the content, occurrence, response and prevention

Valerii Borokhvostov *, Lesia Skurinevska **, Julia Lutsik ***

** Central Research Institute of the Armed Forces of Ukraine,
28, Vozduhoflotsky, ave, Kyiv, 03049, Ukraine,
e-mail: bvk51@ukr.net,
Candidate of Technical Sciences (Ph.D.), Associate Professor,
Leading Researcher.*

*** The National Defence University of Ukraine named after Ivan Cherniakhovskyi,
28, Vozduhoflotsky, ave, Kyiv, 03049, Ukraine,
e-mail: olesya201405@gmail.com,
Candidate of Military Sciences (Ph.D.),
Associate Professor of the Department of Economics and Financial Security.*

**** The National Defence University of Ukraine named after Ivan Cherniakhovskyi,*

28, Vozduhoflotsky, ave, Kyiv, 03049, Ukraine,

e-mail: Julia.Lutsik@gmail.com,

Candidate of Economy Sciences (Ph.D.),

Chief of the Department of Economics and Financial Security.

Abstract: The article studies goals and application methods of information and financial technologies in the so-called hybrid wars, which recently have become actively used by many influential countries in the world. Authors of the article propose scientific and methodological guide and appropriate methods for hybrid wars prompt prevention, detection, analysis and development of responding methods. Authors emphasize that recently world is opted for new, less economically costly mode of warfare rather than wars traditional methods. One of these types of wars is the so-called hybrid wars. This type of war has many aspects, but the authors of this article have focused only on one of them, the interest of which has appeared recently, namely - *information and financial technologies (IFT)* of conducting this type of war.

Based on this, the article discloses the content of the hybrid warfare IFT and main goals pursued by the so-called «aggressor country», and presents developed by the authors general scheme of the scientific and methodological guide for conducting hybrid warfare IFT manifestations research, which consists of the phase of identification of occurrence of the hybrid warfare IFT manifestations and three interrelated methods: methods of analysis of hybrid warfare IFT manifestations; methods of development of responding measures to the manifestations of hybrid warfare IFT; methods for developing and implementing measures to prevent the emergence of hybrid warfare IFT manifestations, etc. Article further outlines the schemes and the detailed content of these methods.

The authors of the article emphasize that in order to counteract the manifestations of hybrid warfare IFT, should be developed the measures aimed to elimination of the consequences of established negative facts, as well as to prevention the occurrence of cases which lead or may lead to their occurrence in the "target country". For this purpose, they are offered purposely deducted methodology, scheme and general content of which are presented in the article. The main which they insist on is that no grounds should be created in the country to accuse country or its authority in financial fraud. That is the only way to prevent the use of hybrid warfare IFT towards the country.

Keywords: hybrid warfare, information company, information and financial technologies, “aggressor country”, “target country”, financial scandal.

Bibliography 2, picture 7

Використана література

1. Югай Т.А. Информационно-финансовые технологии гибридной войны. *Вооружение и экономика* № 4 (37) 2016. С. 113-127.
2. Югай Т.А. «Антикоррупционные» сценарии гибридной войны. *Вооружение и экономика* № 4 (41) 2017. С. 59-75.

References

1. Yugai T. (2016) Informationsionno finansovyye tekhnologii gibridnoy voyny. *Vooruzheniye i ekonomika*. №4 (37) 2016. 113–127.
2. Yugai T. (2017) Anty-corruption stsensarii gibridnoy voyny. *Vooruzheniye i ekonomika* №4 (41) 2017. 59–75.

© 2019 by the authors; Social development & Security, Ukrainian. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CCBY) license (<http://creativecommons.org/licenses/by/4.0/>).