УДК 004.056: 330.34

Яровенко Ганна Миколаївна
кандидат економічних наук, доцент,
доцент кафедри економічної кібернетики
Сумський державний університет
Яровенко Анна Николаевна
кандидат экономических наук, доцент,
доцент кафедры экономической кибернетики
Сумской государственный университет
Yarovenko Hanna
PhD, Associate Professor,
Associate Professor of the Economic Cybernetics Department
Sumy State University
ORCID: 0000-0002-8760-6835

DOI: 10.25313/2520-2294-2020-9-6318

НАСЛІДКИ ІНФОРМАЦІЙНИХ ВІЙН ЯК ФАКТОР ЕКОНОМІЧНОЇ ДЕСТАБІЛІЗАЦІЇ КРАЇНИ

ПОСЛЕДСТВИЯ ИНФОРМАЦИОННЫХ ВОЙН КАК ФАКТОР ЭКОНОМИЧЕСКОЙ ДЕСТАБИЛИЗАЦИИ СТРАНЫ

THE CONSEQUENCES OF INFORMATION WARS AS A FACTOR OF THE COUNTRY ECONOMIC DESTABILIZATION

Анотація. *Наслідки четвертої промислової революції призвели до впровадження потужних кіберфізичних комплексів та сучасного програмного забезпечення у різні сфери діяльності. Але їх розповсюдженість та доступність стали причиною зростання кіберзлочинності у світі та виникненню інформаційних війн, ініціаторами яких виступають різні країни. В результаті це призводить до дестабілізації економічного, політичного та соціального секторів країни та гальмує її розвиток. Мета даного дослідження присвячена аналізу основних показників та наслідків, характерних для інформаційних війн, та розробці підходу до моделювання розповсюдження їх результатів, як факторів економічної дестабілізації країни, у вигляді розриву «інформаційної бульбашки» – ударно-хвильової моделі Сєдова-Тейлора. Так у статті було проведено аналіз ряду основних показників, фактичні дані яких показали, що відбувається постійне збільшення випадків ведення інформаційних війн, які здійснюються однією країною проти інших. Це проявляється у зростанні кількості хакерських кібератак, спрямованих на різні сфери діяльності, розширення можливостей кіберзлочинців, виникненні політичної вмотивованості уряду здійснювати інформаційну пропаганду та кібершпигунство. У роботі було проаналізовано також й основні фінансові наслідки кібервійн у світі, які характеризують зростання глобальних фінансових втрат та втрат для компаній різних секторів економіки. Для підвищення ефективності контролю за наслідками інформаційних війн запропоновано ударно-хвильову модель Сєдова-Тейлора у вигляді розриву «інформаційної бульбашки» для моделювання розповсюдження наслідків інформаційних війн, як фактору економічної дестабілізації країни, для банків, підприємств та держави в цілому. Використання подібних моделей дозволить виявити вразливі місця в системі інформаційної безпеки країни для подальшого формування її стратегії розвитку.*

Ключові слова: *дестабілізація, втрати, економіка, «інформаційна бульбашка», інформаційна війна, кібервійна, модель Сєдова-Тейлора, наслідки.*

Аннотация. *Последствия четвертой промышленной революции привели к внедрению мощных киберфизичних комплексов и современного программного обеспечения в различных сферах деятельности. Но их распространенность*

и доступность стали причиной роста киберпреступности в мире и возникновению информационных войн, инициаторами которых выступают разные страны. В результате это приводит к дестабилизации экономического, политического и социального секторов страны и тормозит ее развитие. Цель данного исследования посвящена анализу основных показателей и последствий, характерных для информационных войн, а также разработке подхода к моделированию распространения их результатов, как факторов экономической дестабилизации страны, в виде разрыва «информационной пузыря» – ударно-волновой модели Седова-Тейлора. Так, в статье был проведен анализ ряда основных показателей, фактические данные которых дали возможность представить, что происходит постоянное увеличение случаев ведения информационных войн, которые осуществляются одной страной в отношении других. Это проявляется в росте числа хакерских кибератак, направленных на различные сферы деятельности, расширении возможностей киберпреступников, возникновении политической мотивированности правительства осуществлять информационную пропаганду и кибершпионаж. В работе проанализированы также и основные финансовые последствия кибервойн в мире, которые характеризуют рост глобальных финансовых потерь и потерь для компаний различных секторов экономики. Для повышения эффективности контроля за последствиями информационных войн предложено использование ударно-волновой модели Седова-Тейлора в виде разрыва «информационного пузыря» для моделирования распространения последствий информационных войн, как фактора экономической дестабилизации страны, для банков, предприятий и государства в целом. Использование подобных моделей позволит выявить уязвимые места в системе информационной безопасности страны для дальнейшего формирования ее стратегии развития.

Ключевые слова: *дестабилизация, потери, экономика, «информационная пузырь», информационная война, кибервойна, модель Седова-Тейлора, последствия.*

Summary. *The consequences of the fourth industrial revolution led to the introduction of robust cyber-physical systems and modern software in various fields of life activity. But their prevalence and availability have caused the growth of cybercrime in the world and the emergence of information wars, initiated by different countries. As a result, it leads to the destabilization of the country's economic, political, and social sectors, and impedes its development. The purpose of this study is to analyze the leading indicators and consequences typical for information wars, as well as to develop an approach to modeling the spread of their results as factors of country economic destabilization, in the form of a bursting of the «information bubble» – the Sedov-Taylor shock wave model. The article analyzed several critical indicators, the factual data of which made it possible to imagine that there is a constant increase in the number of information wars that are carried out by one country against others. It is manifested by the rise in the number of hacker cyberattacks aimed at various areas of activity, the empowerment of cybercriminals, the emergence of the government political motivation to carry out information propaganda, and cyber espionage. The paper also analyzes the main financial consequences of cyberwars globally, which characterize the growth of global economic losses and losses for companies in various sectors of the economy. To increase the effectiveness of control over the consequences of information wars, the author proposed to use the Sedov-Taylor shock-wave model in the form of a burst of the «information bubble» to simulate the spread of the consequences of information wars, as a factor of country economic destabilization, for banks, enterprises and the state as a whole. Such models will make it possible to identify vulnerabilities in the country's information security system for further shaping its development strategy.*

Key words: *destabilization, losses, economy, «information bubble», information war, cyber war, the Sedov-Taylor model, consequences.*

Постановка проблеми. В сучасному світі найбільшого поширення набуває практика інформаційного впливу на різні сфери діяльності, як на рівні держави, так й на глобальному рівні. Влада інформації перетворюється на вирішальну силу при управлінні суспільством, зміщуючи акценти впливу фінансових й політичних державних важелів на другорядний план. Розвиток сучасних інформаційних технологій охопив майже всі галузі суспільної діяльності, в тому числі й мистецтво ведення інформаційних війн. Їх роль протягом останнього десятиліття неухильно зростає, оскільки відмінною їх особливістю є відсутність видимих руйнівних наслідків, а також поступове, майже непомітне втілення в усіх сферах суспільної, політичної та економічної життєдіяльності.

Інформаційна війна — це сучасний вид озброєння, який застосовується різними державами світу з метою дестабілізації певної сфери діяльності в країні. Це відбувається шляхом використання різних інструментів, таких як кібершпигунство, пропаганда, хакерські атаки, веб-вандалізм, викрадення конфіденційної інформації, тощо. Як правило, той, хто застосовує інструменти ведення інформаційної війни, намагається вплинути на конкретний об'єкт та порушити його функціонування або змінити його

відповідно до інших правил, або взагалі зруйнувати. Наслідки від цього можуть бути непередбачуваними та відчутними протягом тривалого періоду часу. Деякі країни створюють спеціальні підрозділи, діяльність яких спрямована на ведення інформаційних війн проти інших держав з метою втручання в їх політичне, соціальне та економічне життя.

Безболісно подолати наслідки інформаційних війн неможливо, оскільки вони здатні проникнути в усі сфери життєдіяльності суспільства та вкрай негативно тиснути на людство. Сторона, що програє в інформаційній війні, може втратити контроль, стати підвладною стороні-переможцю, стикнутися з руйнуванням працездатності економічної системи, порушенням політичної стабільності, знищенням непотрібних переможцю структур, і навіть системи національної безпеки. Але особливо відчутними є наслідки в економічній сфері, оскільки за часту об'єктом кіберзлочинів є фінансова інформація, або втрата інформації може призвести до фінансових втрат.

Відповідно питання захисту від такої зброї повинно бути одним із найвищих пріоритетів для систем національної та світової безпеки. Так, в цьому напрямку Тімом Бернерсом-Лі, творцем Всесвітньої павутини, 25 листопада 2019 року був запропонований «Мережевий контракт», який являє собою план дій для уряду, компаній та окремих осіб щодо захисту в мережі від різного роду інформаційного впливу. Тобто вони повинні узяти на себе обов'язки щодо захисту мережі від різного роду інформаційних фейків, неправдивих політичних новин, порушення конфіденційності та іншого роду зловживань [1].

Також деякі країни створюють спеціальні підрозділи реагування, які займаються виявленням та попередженням ймовірних проявів інформаційних війн. Окрім цього уряд багатьох країн сприяє розробці національної стратегії інформаційного захисту та протидії кібертероризму, організації спеціалізованих органів та інститутів, що діють в цьому напрямку. Сучасні вчені та науковці також звертають увагу на питання протидії інформаційним війнам та намагаються знайти ефективні рішення. У цьому напрямку можна виділити математичний інструментарій, застосування якого дозволяє моделювати ситуації, пов'язані зі здійсненням кібератак, та прогнозуванням наслідків. Роботи подібного характеру спрямовані на створення додаткових заходів, які дозволять виявляти слабкі місця в системах захисту, та надалі вибудовувати ефективну системи інформаційного захисту. Саме тому дослідження, присвячене вирішенню проблеми моделювання розповсюдження наслідків інформаційних війн як фактору економічної дестабілізації країни є актуальним та практично значущим.

Аналіз останніх досліджень і публікацій. Вирішенню проблеми інформаційних війн присвячено багато праць зарубіжних та вітчизняних науковців, які займалися дослідженням їх різних аспектів. Так, Робінсон М., Джонс К. та Яніке Х. намагалися проаналізувати існуючі визначення кібервійни та визначити основні дослідницькі задачі у цій галузі [2]. МакКей Б. та Мунро І. приділили увагу такому аспекту, як використання різних організацій для здійснення інформаційних війн, що призводить до зміну політичних ландшафтів у країні [3]. Кріллі К. розкриває сутність методів, які використовують різні терористичні групи у процесі ведення інформаційної війни, особливо робиться акцент на застосуванні Інтернет-технологій та сучасні засоби комунікації [4]. Дродж К. розглядає правові аспекти, які стосуються захисту прав громадян у випадку ведення інформаційної війни, а також проводить паралелі між даним фактом, війною та озброєним конфліктом [5].

Кенні М. аналізує поняття кібертероризму та формулює основну ідею, що більшість сучасних кібератак не досягають рівня кібертероризму, хоча вони дуже успішно використовуються спеціальними урядовими організаціями для збору інформації, коштів, проведення вербування прибічників, тощо [6]. Кнапп К. Дж. та Боултон В. Р. досліджують основні тенденції стосовно інформаційних війн у світі та наголошують на тому, що вони демонструють перетворення інформаційної війни з політичного та військового інструменту у комерційну проблему, оскільки вони почали активно використовуватися для промислового шпигунства [7]. Окремо слід виділити ідеї Брайанта В. [8] та Кларка Р. [9] стосовно трансформації інформаційних війн у технічні інформаційні атаки та кібервійни.

Особливої уваги заслуговують напрацювання науковців, які стосуються розробки різних інструментів, механізмів та технологій протидії здійснення інформаційних війн та різного роду кібертерористичних атак. Так, Хекман К. Є., Уолш М. Дж., СтехФ.Дж., О'Бойл, Т.А., Дікато С. Р., Гербер А. Ф. представили результати дослідження системи «cyber wargame», яка використовується для тестування платформи кібербезпеки динамічного мережевого захисту, яка дозволяє надавати зловмисникам неправдиву інформацію замість реальної [10]. Місра С., Сінгх Р., Рохіт Мохан С. В. запропонували спеціальний механізм виявлення кібератак з використанням радіоперешкод для бездротових мереж [11]. Дудду В. досліджує напрямки застосування методів

інтелектуального аналізу з метою протидії кібератакам та інформаційному тероризму та розглядає різні методи захисту у відповідністю із моделями загроз для систем машинного навчання [12].

Хоча вирішенню проблеми «інформаційних війн» приділено значну увагу з боку дослідників, економістів та вчених, але в науковій літературі й досі відсутня чітка методика подолання такої серйозної загрози.

Мета статті полягає у проведенні аналізу основних показників та наслідків, притаманних інформаційним війнам, та розробці підходу до моделювання розповсюдження результатів інформаційних війн, як факторів економічної дестабілізації країни, у вигляді розриву «інформаційної бульбашки» — ударно-хвильової моделі Сєдова-Тейлора.

Виклад основного матеріалу. Поняття «інформаційна війна» є широким та охоплює діяльність спеціалізованих угрупувань або окремих осіб, яка набуває значних масштабів та спрямована на викрадення інформації, її викривлення, порушення цілісності, використання у злочинних цілях, тощо. Основними інструментами інформаційної війни є масові хакерські кібератаки, кібершпигунство, інформаційна пропаганда, вірусні атаки з метою збору конфіденційної інформації, централізовані атаки на сервери, мережі, підробка кодів, програмного, технічного забезпечення, пристроїв введення-виведення, тощо. Крім цього можна виділити ряд показників, які дозволяють оцінити масштаби ведення інформаційних війн та зрозуміти вплив цього явища на життєдіяльність країни та світу в цілому. Так, на рисунку 1 представлена інфографіка таких показників, яку було складено із використанням програмного продукту «VISME» на основі статистичних даних, зібраних міжнародними організаціями та аналітиками.

Кожні 39 секунд у світі відбувається кібератака, що говорить про масовість та розповсюдженість

Рис. 1. Інфографіка основних показників інформаційних війн

Джерело: побудовано автором на основі [13; 14; 15]

даного явища (рисунок 1). Це пов'язано із зростанням технічних можливостей для кіберзлочинців та доступністю різних пристроїв для хакерів, мінімальна ціна за які складає 1 долар. Тільки у 2018 році компанія Cisco заблокувала 7 трлн. загроз, що складає близько 20 млрд. загроз на день [13]. Кіберзлочини поступово набувають масового характеру, оскільки пов'язані із відносною простотою здійснення та за часту уникненням відповідальності за рахунок існування часового лагу між здійсненням та виявленням. Статистика для США показує, що вони складають близько 10–12% від загального обсягу злочинів (рисунок 1). Їх мета може бути різною, хоча близько 11% кібератак пов'язують саме із кібершпигунством, що дозволяє ряду країн викрадати секретні дані, які використовуються проти інших, або приводять до дисбалансу в політичній чи економічні сферах. Так, близько 26,3% ударів кібервійн спрямовані проти США, при чому доля Китаю в цьому складає 31,6% [13]. Лідерами в галузі ведення кібервійн проти інших країн є Китай та Росія, хоча Іран, США, Великобританія та ряд інших країн щільно займаються цим питанням (рисунок 1).

Окрім цього можна виділити таку форму інформаційної війни, як промислове кібершпигунство, яке направлене на підрив діяльності крупних компаній. Найбільшими жертвами в цьому є підприємства роздрібної торгівлі, IT-компанії та уряд (рисунок 1), хоча промислові компанії та фінансово-кредитні установи за показниками інформаційних атак також наближаються до лідерів. Це пов'язано не тільки з тим, що діяльність злочинців спрямована на викрадення фінансової інформації саме цих важливих для економіки об'єктів, але й це відбувається за рахунок слабкої організації їх систем захисту. Даний

Рис. 2. Інфографіка основних фінансових наслідків інформаційних війн

Джерело: побудовано автором на основі [13; 14; 15]

фактор є характерним для більшості компаній світу та у випадку зберігання подібної тенденції це може призвести до важких фінансових наслідків не тільки для них, але й для економіки країни в цілому. Так, на рисунку 2 представлено інфографіку основних фінансових наслідків, отриманих в результаті здійснення інформаційних війн.

Фінансові втрати від кібервійн по всьому світу склали 0,8% від світового ВВП у 2018 році. При цьому прогнозується зростання збитків у геометричній прогресії, що буде складати щорічно близько 6 трлн. дол. у 2021 році (рисунок 2). На долю Азіатсько-Тихоокеанського регіону припадає близько 1,745 трлн. дол. економічних втрат, що говорить про зростання його важливості для кіберзлочинців, оскільки сьогодні в багатьох країнах даного регіону зосереджені великі IT-компаніїї та нафтові підприємства. Набуває популярності кібершахрайства із криптовалютами. Так, було виявлено близько 76 млрд. доларів незаконних операцій із криптовалютою, що наближається за світовими обсягами до незаконних операцій із наркотиками [13]. Окрім цього набувають поширення кіберзлочини, які здійснюються за допомогою цифрової реклами, що прогнозується досягти 44 млрд. доларів у 2022 році [13]. Як правило, дані операції призводять до легалізації цих коштів, що врешті-решт негативно впливає на розвиток економіки.

Країнами світу ведеться боротьба із наслідками інформаційних війн, що полягає у посиленні заходів із інформаційної безпеки в цілому та кібербезпеки зокрема. Так, у 2019 році світові витрати на захист інформації склали 124 млрд. дол., що перевищує їх суму у 2018 році (114 млрд. дол.). Прогнозується зростання даної суми у 2022 році до 170,4 дол. [13]. Окрім цього можна виділити таку проблему, як неякісне програмне забезпечення для захисту даних. У 2021 році світові втрати від його функціонування склали 20 млрд. дол., що перевищило даний показник у попередні роки практично у 2 рази (рисунок 2). Також зростають витрати компаній на підготовку фахівців у галузі захисту інформації. Прогнозується збільшення даного показника до 10 млрд. дол. у 2027 році, в порівнянні з 1 млрд. дол. у 2014 році [13]. При цьому негативні аспекти від впливу кібервійн проявляються також й в тому, що компанії мають проблеми, пов'язані із подальшою їх діяльністю. Тобто багатьом з них (60%) дуже важко відновлювати інформацію та продовжувати свою роботу на попередньому рівні (рисунок 1). Особливо це проблематично для малих підприємств.

Таким чином, інформаційні війни здійснюють вплив на різні сфери діяльності та результатом цього, як правило, є зростання фінансових збитків та витрат, пов'язаних із підвищенням ефективності систем захисту. Дана проблема потребує знаходження універсальних підходів, реалізація яких дозволила б спрогнозувати потенційні результати для окремої країни, отримані в процесі реалізації інформаційних війн. Саме тому пропонуємо використовувати підхід ударної хвилі, який дозволить сприймати виникнення наслідків кібервійн у якості «інформаційних бульбашок».

«Інформаційною бульбашкою» є певна подія, яка непередбачувана та відбувається не на постійній основі, але її виникнення призводить до конкретних результатів, за часту до збільшення негативних наслідків протягом певного часу. У якості такої «бульбашки» може виступати один із напрямів інформаційної війни, наприклад, хакерська атака. Наслідки від цього можуть зростати у геометричній прогресії аж до економічної дестабілізації країни. Специфічні особливості та масштаби виникнення «інформаційних бульбашок», як негативних наслідків інформаційних війн, в свою чергу, визначають вектори поширення в економічній та соціальній сферах та впливають на різні канали їх поширення. Все це формує передумови для можливої математичної формалізації розповсюдження наслідків інформаційних війн, як факторів економічної дестабілізації країни, у вигляді розриву «інформаційної бульбашки» — ударно-хвильової моделі Сєдова-Тейлора. Застосування зазначеного підходу до моделювання полягає у доцільності формуванні основної гіпотези щодо наявності «інформаційних бульбашок» та їх розривів, як передвісників процесів економічної дестабілізації країни в розрізі інформаційного поля.

Модель Сєдова-Тейлора [16, 17], яка дозволяє описати ударну хвилю, має вигляд:

$$R_s(t) = a \cdot t^b ,$$

$$b = \frac{s+2}{n+2} , \; a = \left(\frac{E_d / \left(\tau_0^s l_0^{3-n} \right)}{\rho} \right)^{1/(n+2)} , \qquad (1)$$

де n — просторовий вимір (n=1 для плоского простору, n=2 для циліндричного простору, n=3 для сферичного простору);

s — фактор швидкості виділення енергії (s=0 для випадку миттєвого виділення, s=1 для випадку виділення з постійною швидкістю);

E_d — енергія, що виділяється при детонації і має наступні характеристики: l_0 — довжина, τ_0 — час;

ρ — щільність атмосферного повітря.

Адаптуємо формулу (1) для опису моделі ударної хвилі розповсюдження наслідків інформаційних

війн, як факторів дестабілізації економіки країни. Оскільки при описі соціально-економічної системи втрачає сенс просторова характеристика, кожен спектр вертикального (макро- та мікрорівень) та горизонтального (банків та суб'єктів господарської діяльності) секторів буде мати власний канал розповсюдження, а замість просторових характеристик виникає необхідність використання фактору часу. Запишемо формулу, яка дозволить кількісно описати «тиск» ударної хвилі розриву «інформаційної бульбашки» та тенденцію його згасання, що супроводжує процес послідовного розсіювання енергії — проявів та каналів економічної дестабілізації країни. Модель Сєдова-Тейлора з урахуванням адаптації набуває вигляду [18]:

$$\Delta R(t) = \frac{E}{t^4} + a_1\left(\frac{E}{t^4}\right)^{3/4} + a_2\left(\frac{E}{t^4}\right)^{2/4} + a_3\left(\frac{E}{t^4}\right)^{1/4}, \quad (2)$$

де $\Delta R(t)$ — зменшення втрат інформації, порушень у системі безпеки, що виражається або у кількості записів для втрат, або у кількості випадків порушень, що відбуваються за період t;

E — енергія в початковий момент після розриву бульбашки, що в нашому випадку пропонується інтерпретувати як дохід (або прибуток), пов'язаний із втратою інформації чи порушень системи захисту;

t — період часу після розриву «інформаційної бульбашки» (кількість місяців);

a_1, a_2, a_3 — характеристики середовищ поширення ударних хвиль наслідків інформаційних війн.

Оскільки виникає необхідність мінімізації втрат інформації або мінімізації випадків порушення інформаційної безпеки (кількість записів або кількість випадків), що виступають однією із форм прояву «інформаційної війни», розглянемо модель Сєдова-Тейлора з точки зору оптимізаційної задачі нелінійного програмування. Для цього в розрізі кожного із напрямків дестабілізації економіки країни необхідно ідентифікувати «вид інформаційної війни» та відповідно розрив «інформаційної бульбашки», яка буде характеризувати ударну хвилю, що виникла та повинна поступово розсіятися. Таким чином, параметри моделі (2) мають забезпечити мінімально можливий рівень втрат інформації або випадків порушення інформаційної безпеки (кількості записів або кількості випадків) для кожного прояву дестабілізації економіки країни, тобто в банківській сфері, для підприємств, держави в цілому. Враховуючи наведені аргументи, оптимізаційна задача моделювання розповсюдження наслідків інформаційних війн, як фактору економічної дестабілізації країни, з урахуванням різних їх проявів та каналів набуває вигляду (формула 3):

$$\begin{cases} U_i \to \min \\ U_i = \sum_{j=1}^{V} U_{ij}^{t_j} = \\ = \sum_{j=1}^{V}\left(\frac{z_{t_j}^i}{\tau_j^i} + a_1\left(\frac{z_{t_j}^i}{\left(\tau_j^i\right)^2}\right)^{3/4} + a_2\left(\frac{z_{t_j}^i}{\left(\tau_j^i\right)^3}\right)^{2/4} + a_3\left(\frac{Ez_{t_j}^i}{\left(\tau_j^i\right)^4}\right)^{1/4}\right) \end{cases} \quad (3)$$

де U_i — розсіювання енергії ударної хвилі в i-му каналі поширення економічної дестабілізації країни, тобто для банків, підприємств, держави в цілому;

V — кількість видів інформаційних війн (хакерські атаки, кібершпигунство, інформаційна пропаганда, тощо);

$z_{t_j}^i$ — значення початкової енергії в момент часу t_j, тобто початкові значення доходів (прибутків) для відповідних каналів поширення до початку здійснення інформаційної війни;

t_j — момент часу початку j-ого виду інформаційної війни в i-му напрямку дестабілізації економіки країни;

τ_j^i — тривалість j-ого виду інформаційної війни в i-му напрямку дестабілізації економіки країни.

Застосування формули 3 дозволить змоделювати ситуацію розповсюдження наслідків різних видів інформаційних війн, які проявляються у вигляді фінансових втрат для підприємств, банків, держави та врешті решт призводять до економічної дестабілізації країни.

Висновки та перспективи подальших досліджень. На сучасному етапі розвитку суспільства для вирішення соціальних, політичних, економічних проблем та конфліктів все частіше вдаються до використання можливостей інформаційного простору. Одним із напрямів цього є ведення інформаційних війн, які застосовуються, як правило, для реалізації дій злочинного характеру, що призводить до появи багатьох несприятливих наслідків для тієї країни, по відношенню до якої було вживано дані заходи. У статті зазначено, що інструментами ведення таких війн є хакерські кібератаки, кібершпигунство, пропаганда та інші, мета застосування яких пов'язана із викраденням, викривленням, знищенням інформації «потенційного» противника. Також було проаналізовано ряд показників, які характеризують інформаційні війни. Їх статистичні значення свідчать про зростання даної проблеми у всьому світі, що говорить про можливості виникнення озброєних конфліктів між країнами, як наслідки ведення інформаційних війн між ними. У роботі було проаналізовано також й основні фінансові наслідки, отримані в результаті

кібервійн у світі. Їх прогнозні значення свідчать не тільки про зростання втрат в майбутньому, а також й про збільшення витрат на забезпечення системи інформаційної безпеки. Тобто при відсутності дієвих заходів захисту та зростаючих можливостях для кіберзлочинців прогнозується в цілому несприятлива ситуація у світі, яка буде пов'язана із дестабілізацією різних сфер життєдіяльності, особливо економічної.

Для встановлення контролю за ходом інформаційних війн та управління ними, розробляються певні методики та моделі. Так, в роботі пропонується застосовувати ударно-хвильову модель Сєдова-Тейлора у вигляді розриву «інформаційної бульбашки» для моделювання розповсюдження наслідків інформаційних війн, як фактору саме економічної дестабілізації країни з урахуванням різних факторів. Дану модель було адаптовано під умови розповсюдження наслідків для таких каналів, як банки, підприємства та держава. Подібні моделі є формою інформаційною зброї, що здатна надати максимальний ефект, оскільки допомагає виявити ряд загрозливих чинників дестабілізації держави, встановити найбільш вразливі ділянки системи, та спрогнозувати потенційні варіанти розвитку подій, щоб мати можливість завчасно передбачити можливі негативні наслідки інформаційних війн.

В наступному дослідженні планується здійснити розрахунки із використанням запропонованої адаптованої моделі на основі емпіричних даних щодо інформаційних втрат (випадків порушення інформаційної безпеки) та прибутків, пов'язаних із діяльністю банків, підприємств та держави.

Робота виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України».

Література

1. Launching the Contract for the Web // World Wide Web Foundation: веб-сайт. URL: https://webfoundation.org/2019/11/launching-the-contract-for-the-web/ (дата звернення: 29.09.2020).

2. Robinson M., Jones K., Janicke H. Cyber warfare: Issues and challenges // Computers and Security. 2015. Vol. 49. PP. 70–94. DOI: 10.1016/j.cose.2014.11.007.

3. MacKay B., Munro I. Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil-Greenpeace Dispute over Climate Change // Organization Studies. 2012. Vol. 33. Issue 11. PP. 1507–1536. DOI: 10.1177/0170840612463318.

4. Crilley K. Information warfare: New battlefields Terrorists, propaganda and the Internet // Aslib Proceedings. 2001. Vol. 53. Issue 7. PP. 250–264. DOI: 10.1108/EUM0000000007059.

5. Droege C. Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians // International Review of the Red Cross. 2013. Vol. 94. Issue 886. PP. 533–578. DOI: 10.1017/S1816383113000246.

6. Kenney M. Cyber-Terrorism in a Post-Stuxnet World // Orbis. 2015. Vol. 59. Issue 1. PP. 111–128. DOI: 10.1016/j.orbis.2014.11.009.

7. Knapp K.J, Boulton W. R. Cyber-warfare threatens corporations: Expansion into commercial environments // Information Systems Management. 2006. Vol. 23. Issue 2. PP. 76–87. DOI: 10.1201/1078.10580530/45925.23.2.20060301/92675.8.

8. Bryant W. D., 2013. Cyberspace superiority. A conceptual model. Air & Space Power Journal, 29(2), pp. 103–128.

9. Budanović N., 2020. The largest battlefield in history — 30 Cyber warfare statistics. DataProt.. [Online] Available at: https://dataprot.net/statistics/cyber-warfare-statistics/ [Accessed 29 09 2020].

10. Clarke R. A., 2010. Cyber war. The next threat to national security and what to do about it. New York: Ecco. 290 pp..

11. Crilley K., 2001. Information warfare: New battlefields Terrorists, propaganda and the Internet. Aslib Proceedings, 53(7), pp. 250–264. DOI: 10.1108/EUM0000000007059.

12. Droege C., 2013. Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), pp. 533–578. DOI: 10.1017/S1816383113000246.

13. Duddu V., 2018. A survey of adversarial machine learning in cyber warfare. Defence Science Journal, 68(4), pp. 356–366.

14. Heckman K. E., Walsh M. J., Stech F. J., O'Boyle T.A., Dicato S. R., Herber A. F., 2013. Active cyber defense with denial and deception: A cyber-wargame experiment. Computers and Security, Volume 37, pp. 72–77. DOI: 10.1016/j.cose.2013.03.015.

15. Kenney M., 2015. Cyber-Terrorism in a Post-Stuxnet World. Orbis, 59(1), pp. 111–128. DOI: 10.1016/j.orbis.2014.11.009.

16. Knapp K.J, Boulton W. R., 2006. Cyber-warfare threatens corporations: Expansion into commercial environments. Information Systems Management, 23(2), pp. 76–87. DOI: 10.1201/1078.10580530/45925.23.2.20060301/92675.8.

17. MacKay B., Munro I., 2012. Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil-Greenpeace Dispute over Climate Change. Organization Studies, 33(11), pp. 1507–1536. DOI: 10.1177/0170840612463318.

18. McAfee, 2018. Economic Impact of Cybercrime — No Slowing Down. [Online] Available at: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/mcafee/economic-impact-of-cybercrime-not-slowing-down.pdf [Accessed 29 09 2020].

19. Misra S., Singh R., Rohith Mohan S. V., 2010. Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Sensors, 10(4), pp. 3444–3479. DOI: 10.3390/s100403444.

20. Morgan S., 2019. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Cybercrime Magazine. [Online] Available at: https://cybersecurityventures.com/cybersecurity-almanac-2019/[Accessed 29 09 2020].

21. Robinson M., Jones K., Janicke H., 2015. Cyber warfare: Issues and challenges. Computers and Security, Volume 49, pp. 70–94. DOI: 10.1016/j.cose.2014.11.007.

22. World Wide Web Foundation, 2019. Launching the Contract for the Web. [Online] Available at: https://webfoundation.org/2019/11/launching-the-contract-for-the-web/ [Accessed 29 09 2020].

References

1. Launching the Contract for the Web. World Wide Web Foundation. Available at: https://webfoundation.org/2019/11/launching-the-contract-for-the-web/ (accessed 29 September 2020).

2. Robinson M., Jones K., Janicke H. (2015) Cyber warfare: Issues and challenges. Computers and Security, vol. 49, pp. 70–94. DOI: 10.1016/j.cose.2014.11.007.

3. MacKay B., Munro I. (2012) Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil-Greenpeace Dispute over Climate Change. Organization Studies, 33(11), pp. 1507–1536. DOI: 10.1177/0170840612463318.

4. Crilley K. (2001) Information warfare: New battlefields Terrorists, propaganda and the Internet. Aslib Proceedings, 53(7), pp. 250–264. DOI: 10.1108/EUM0000000007059.

5. Droege C. (2013) Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), pp. 533–578. DOI: 10.1017/S1816383113000246.

6. Kenney M. (2015) Cyber-Terrorism in a Post-Stuxnet World. Orbis, 59(1), pp. 111–128. DOI: 10.1016/j.orbis.2014.11.009.

7. Knapp K.J, Boulton W. R. (2006) Cyber-warfare threatens corporations: Expansion into commercial environments. Information Systems Management, 23(2), pp. 76–87. DOI: 10.1201/1078.10580530/45925.23.2.20060301/92675.8.

8. Bryant W. D., 2013. Cyberspace superiority. A conceptual model. Air & Space Power Journal, 29(2), pp. 103–128.

9. Budanović N., 2020. The largest battlefield in history — 30 Cyber warfare statistics. DataProt.. [Online] Available at: https://dataprot.net/statistics/cyber-warfare-statistics/[Accessed 29 09 2020].

10. Clarke R. A., 2010. Cyber war. The next threat to national security and what to do about it. New York: Ecco. 290 pp.

11. Crilley K., 2001. Information warfare: New battlefields Terrorists, propaganda and the Internet. Aslib Proceedings, 53(7), pp. 250–264. DOI: 10.1108/EUM0000000007059.

12. Droege C., 2013. Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), pp. 533–578. DOI: 10.1017/S1816383113000246.

13. Duddu V., 2018. A survey of adversarial machine learning in cyber warfare. Defence Science Journal, 68(4), pp. 356–366.

14. Heckman K. E., Walsh M. J., Stech F. J., O'Boyle T.A., Dicato S. R., Herber A. F., 2013. Active cyber defense with denial and deception: A cyber-wargame experiment. Computers and Security, Volume 37, pp. 72–77. DOI: 10.1016/j.cose.2013.03.015.

15. Kenney M., 2015. Cyber-Terrorism in a Post-Stuxnet World. Orbis, 59(1), pp. 111–128. DOI: 10.1016/j.orbis.2014.11.009.

16. Knapp K.J, Boulton W. R., 2006. Cyber-warfare threatens corporations: Expansion into commercial environments. Information Systems Management, 23(2), pp. 76–87. DOI: 10.1201/1078.10580530/45925.23.2.20060301/92675.8.

17. MacKay B., Munro I., 2012. Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil-Greenpeace Dispute over Climate Change. Organization Studies, 33(11), pp. 1507–1536. DOI: 10.1177/0170840612463318.

18. McAfee, 2018. Economic Impact of Cybercrime — No Slowing Down. [Online] Available at: https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/mcafee/economic-impact-of-cybercrime-not-slowing-down.pdf [Accessed 29 09 2020].

19. Misra S., Singh R., Rohith Mohan S. V., 2010. Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Sensors, 10(4), pp. 3444–3479. DOI: 10.3390/s100403444.

20. Morgan S., 2019. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Cybercrime Magazine. [Online] Available at: https://cybersecurityventures.com/cybersecurity-almanac-2019/ [Accessed 29 09 2020].

21. Robinson M., Jones K., Janicke H., 2015. Cyber warfare: Issues and challenges. Computers and Security, Volume 49, pp. 70–94. DOI: 10.1016/j.cose.2014.11.007.

22. World Wide Web Foundation, 2019. Launching the Contract for the Web. [Online] Available at: https://webfoundation.org/2019/11/launching-the-contract-for-the-web/ [Accessed 29 09 2020].