УДК 316.485.26+355.48]:316.776.23
Леся Качковська,
кандидат історичних наук, доцент кафедри музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності,
Волинський національний університет імені Лесі Українки,
kachkovska.lesja@vnu.edu.ua
ORCID ID: 0000-0003-3206-1580;

Галина Малеончук,
кандидат історичних наук, доцент кафедри історії України та археології,
Волинський національний університет імені Лесі Українки,
maleonchuk.galyna@vnu.edu.ua
ORCID ID: 0000-0001-5078-4622;

Дмитро Зінюк,
магістр спеціальності 029 Інформаційна, бібліотечна та архівна справа,
Волинський національний університет імені Лесі Українки.
yulia.bilyak15@gmail.com
DOI 10.29038/2524-2679-2022-03-87-102

ІНФОРМАЦІЙНИЙ ВПЛИВ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

У статті висвітлено вплив інформації в умовах гібридної війни в контексті політичних подій в Україні та на Заході впродовж 2014–2021 рр. Охарактеризовано інформацію як особливий засіб ведення війни. Також звернено вагу на фейки як загрозу для інформаційної безпеки, зокрема для України. Визначено, що основними цілями інформаційної політики України є забезпечення захисту інформаційного суверенітету (особливо захист національного інформаційного простору з інформаційним ресурсом та систем формування масової суспільної свідомості) в сучасних умовах глобалізації та інтернаціоналізації процесів в інформаційній сфері. Важливою складовою частиною держави є підвищена увага до рівня інформаційної достатності для прийняття рішень публічними органами, підприємствами й громадянами; реалізації конституційних прав і свобод громадян, суспільства. Проаналізовано діяльність вітчизняних органів державної влади стосовно захисту інформаційного простору від внутрішніх та зовнішніх загроз.

З'ясовано, що Верховна Рада України як орган законодавчої влади приймає закони, котрі регулюють стосунки в галузі інформаційної безпеки й захисту інформації. Нормативну базу формують на основі нормативних правових актів у галузі інформації, що видають органи різних гілок влади. Органи виконавчої влади (Кабінет Міністрів України), до складу якого входять міністерства з підпорядкованими їм органами, місцеві органи виконавчої влади виконують відповідні закони. Підкреслено, що система визначень, котра характеризує різні аспекти інформаційної діяльності, стає основою формування відповідних безпекових понять, необхідних для розвитку технологій організації та забезпечення інформаційної безпеки. Результатом наукового дослідження є висновки, які висвітлюють аналіз змісту складників, зокрема комплекс нормативних документних ресурсів і публікацій щодо інформаційної агресії на Україну з боку російської федерації.
Ключові слова: інформація, інформаційна безпека, гібридна війна, фейки, загроза, вплив, суспільство.

Lesia Kachkovska,
Lesya Ukrainka Volyn National University,
ORCID ID: 0000-0003-3206-1580;

Halyna Maleonchuk,
Lesya Ukrainka Volyn National University,
ORCID ID: 0000-0001-5078-4622;

Dmytro Ziniuk,
Lesya Ukrainka Volyn National University

INFORMATION INFLUENCE IN THE CONDITIONS OF HYBRID WARFARE

The article highlights the influence of information in the conditions of hybrid warfare in the context of political events in Ukraine and the West for the period of 2014–2021. Information is defined as a special means of waging war. Attention is also paid to fakes as a threat to information security, in particular for Ukraine. It was determined that the main goals of the information policy in Ukraine are the following to ensure the protection of information sovereignty (especially the protection of the national information space with information resources and systems for the collective social consciousness formation) in modern conditions of globalization and internationalization of processes in the information sphere. An important component of the state is an increased attention to the level of informa-

tion sufficiency for decision-making by public bodies, enterprises and citizens as well as realization of constitutional rights and freedoms of citizens and society. The activities of domestic state authorities in protecting the information space from internal and external threats are analyzed. It was found that the Verkhovna Rada of Ukraine, as a body of legislative power, adopts laws regulating relations in the field of information security and information protection. The regulatory framework is formed using normative legal acts in the field of information issued by the government bodies of various branches. Both bodies of the executive power such as Cabinet of Ministers of Ukraine, which includes ministries with their subordinate bodies and local bodies, execute the relevant laws. It is emphasized that the system of definitions characterizing various aspects of information activities, becomes the basis for the formation of appropriate security concepts necessary for the development of technologies of organization and providing information security. The result of the research is the conclusions that cover the analysis of the components content, in particular, a set of normative document resources and publications on information aggression against Ukraine by the Russian Federation.

Key words: information, information security, hybrid warfare, fakes, threat, influence, society.

1. ВСТУП

Постановка проблеми. Технологічна революція сприяла появі терміна «інформаційна ера», оскільки інформаційні системи стали частиною нашого життя й змінили його докорінно. Сучасний період також вплинув на спосіб ведення бойових дій, забезпечивши командирів безпрецедентною кількістю та якістю інформації.

Потрібно розрізняти війну інформаційної ери й інформаційну війну. Перша використовує інформаційну технологію як засіб для успішного проведення бойових операцій. Технології інформаційної ери реалізували теоретичну можливість – пряме маніпулювання інформацією противника. Інформаційна війна, навпаки, розглядає інформацію як окремий об’єкт або потенційну зброю для безпосереднього досягнення поставленої мети.

Інформаційні війни в сучасному світі певною мірою є формами соціальної взаємодії різних суб’єктів глобалізації, які керуються у своїх діях стандартами відповідних моделей. Саме тому дія й життєздатність процесів глобалізації передбачають класифікацію агресивних інформаційних впливів з урахуванням їх характеру, спрямованості та адресності.

Сучасні вітчизняні й західноєвропейські наукові уявлення про інформаційні війни ще далекі від повноти та ясності. У науковій

літературі й інтернеті розгорнуто велику дискусію з приводу генезису інформаційних війн, характеру та способів їх здійснення. Потрібне також вироблення єдиної методології аналізу їхніх теоретичних, прикладних і суто інформаційних «складових частин».

Система визначень, що характеризує різні аспекти інформаційної діяльності, стає основою формування відповідних безпекових понять, необхідних для розвитку технологій організації й забезпечення інформаційної безпеки. Зокрема, це законодавчі документи: «Про затвердження Зводу відомостей, що становлять державну таємницю» [1], «Про захист інформації в інформаційно-телекомунікаційних системах» [2], «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [3], «Про інформацію» [4], «Положення про Центр протидії дезінформації» [5], «Про основи національної безпеки України» [6], «Про Службу безпеки України» [7], «Про Національну поліцію» [8], «Про стратегію національної безпеки України» [9] та «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» [10].

Мета роботи – на основі системного аналізу дослідити інформацію як об’єкт суспільних відносин, зокрема як засіб ведення інформаційної війни в сучасних умовах.

Методика дослідження. В основу дослідження покладено принципи об’єктивності, науковості, усебічності, системності, які в сукупності дали змогу охарактеризувати способи створення та поширення інформації в умовах гібридної війни, протидію фейковим даним, напрями державної політики тощо.

Методологічну основу становлять загальнонаукові методи аналізу, синтезу, абстрагування та узагальнення. Так, метод аналізу дав змогу охарактеризувати й оцінити джерела дослідження (закони, підзаконні нормативно-правові документи), котрі безпосередньо стосуються зазначеної теми. Залучено також структурно-системний метод, який дав змогу розглянути об’єкт дослідження з усіма його основними рисами як єдине ціле.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Керівництво європейських держав укладає трильйони доларів у створення інформаційних інфраструктур, які можна інтерпретувати, легко отримати до них доступ та використовувати. Такі атрибути, як відкритість і легкість взаємозв’язку систем, що сприяють підвищенню ефективності

й оперативного обслуговування споживачів, є тими самими факторами, які роблять ці системи вразливими до атак. Недавні кібератаки в США підкреслюють це.

Інформаційні воїни вивели загрозу з абстрактної сфери та зробили її реальною. Отже, головним викликом для національних урядів протягом наступного десятиліття буде пошук шляхів захисту оборонної інфраструктури та захист телекомунікаційної комерції під час збереження відкритого суспільства, що здійснюється законними способами. Щоб бути актуальними сьогодні, норми сучасного міжнародного права повинні чітко визначити критерії, що застосовуються для розрізнення того, які дії держави допустимі для легітимних комп'ютерних транскордонних потоків даних для міжнародних комунікацій, торгівлі й фінансової допомоги від тих кіберзаходів, що можуть кваліфікуватися як «збройний напад», проти яких застосовується допустима сила. Навіть із новими формами комп'ютерної зброї та зміною концепцій суверенітету й територій міжнародне право продовжуватиме покладатися на принципи Статуту Організації Об'єднаних Націй та правила для визначення правових меж «кіберпростору». Сучасна державна практика ґрунтується на цих нормах, і вони залишаються основою для керівництва міждержавною поведінкою в епоху інформації [11].

Взаємозв'язок у всьому світі через масивні комп'ютерні мережі робить держави вразливими до нових загроз. Іноземні уряди можуть розпочати комп'ютерні напади або акти інформаційної війни на внутрішні системи іншої держави, такі як енергетичні мережі, телекомунікації та фінансові об'єкти, котрі можуть серйозно пошкодити або порушити національну оборону чи життєво важливі соціальні служби [12].

Оскільки світовий вибух інформаційних технологій, уключаючи обчислювальну техніку, телекомунікації та мережі, змінює спосіб ведення бізнесу, управління й освіти, це обіцяє змінити спосіб боротьби. Інформаційні технології поширюються практично на всю військову сферу, засоби зв'язку, системи управління, а також цивільні системи, що підтримують сучасну промислову (або постіндустріальну) економіку та їх військові зусилля. Деякі з нових способів боротьби позначені як «інформаційна війна», що в цілому було визначено як «будь-які дії з метою заперечення, експлуатації, корупції або знищення інформації та функцій ворога; захист від цих дій; функції військової інформації» [13].

Отже, інформаційна війна включає як нові техніки, такі як вторгнення, злом комп'ютерів і підробка телекомунікацій, так і старі, такі як хитрощі, маскування та фізичні напади на спостережні пункти й лінії

зв'язку. Деякі вважають, що інформаційна війна може розпочати епоху безкровних конфліктів; битва відбуватиметься в «кіберпросторі», оскільки «інформаційні воїни» зможуть вивести з ладу важелі командування та управління противника або цивільну інфраструктуру з незначними людськими втратами. Інші ж припускають, що інформаційні технології можуть сприяти розвитку нових форм соціальної організації, поряд із новими формами конфліктів [14].

Незалежно від розвитку й розповсюдження інформаційних технологій для майбутніх війн, очевидно, що деякі нові форми нападів, які дають інформаційні технології, можуть якісно відрізнятися від попередніх форм нападів. Наприклад, використання таких інструментів, як уторгнення в комп'ютер та комп'ютерні віруси, може вивести війну з фізичного, кінетичного світу та перевести його в нематеріальний, електронний. Ці новіші форми атак, деякі з яких можуть здатися продуктами наукової фантастики, розповсюджуються за континуумами [15].

Напади можуть проводитися здалеку, через радіохвилі або міжнародні комунікаційні мережі, без фізичного вторгнення за межі ворога. Шкода може варіюватися від загибелі військових чи цивільних, від збоїв у роботі системи, до відмови в обслуговуванні важливих військових або державних систем під час кризи, до широкого страху, економічних труднощів або просто незручностей для цивільного населення, яке в повсякденному житті залежить від інформаційних систем.

Сучасна інформаційна війна значною мірою заснована на використанні інформаційних технологій. Із таким використанням виникає залежність, яка створює вразливості, що можуть бути атаковані й повинні бути захищені. Процес нападу на інформаційного супротивника та вразливості інформаційних технологій для будь-якої політичної чи військової структури, захист власної інформації та інформаційних технологій є змістом інформаційної війни [16].

Характер інформаційної війни додатково визначається якостями самих інформаційних технологій: має свої правила й обмеження, засновані на унікальних рисах інформаційних технологій; відсутність чітко відокремлених систем у традиційному розумінні; залежність від комерційних технологій, доступних для більшості людей [17].

Потрібно зазначити, що деякі характеристики інформаційних технологій також можуть внести можливі зміни в організаційну структуру способу придбання таких систем або послуг. Можна перейти до децентралізованої системи, де користувачі визначають власні вимоги, і тоді місцеві інформаційні технології переважно можуть купувати,

установлювати й підтримувати власне обладнання та послуги для задоволення потреб власного користувача в інформаційній війні. Сприяння діяльності, яка уможливлює цей тип децентралізації, може бути ключовою у світі придбання [18].

Інформаційна війна зазвичай має дві поверхні – цивільну та військову. Обидві мають власний діапазон кожної дії, що виконується для отримання інформаційного панування, а також у впливі на деякі процеси, засновані на передачі інформації. Аналіз таких питань обмежується здебільшого через те, що основна територія дій «такої війни» – як вона є, описується військовою й секретною складовою [19].

Сьогодні багато хто вважає, що світ перебуває на передовій однієї з цих періодичних змін у фундаментальній війні – що ми перебуваємо в розпалі так званої військово-технологічної революції (далі – ВТР), яка може спричинити революцію у військовій справі. Технологічні зміни, що покладені в основу сучасної ВТР, складаються переважно з приголомшливих досягнень електронних та інформаційних технологій, які в сукупності доповнюються підвищенням точності, дальності та летальності звичайної зброї.

Оскільки військові переходять до інформаційної війни, досягнення в галузі електронних та інформаційних технологій є лише першим кроком у виконанні ВТР із питань інформаційної війни. Такі військові революції можна вважати чотирма основними елементами, кожен із яких повинен відбутися для досягнення військово-технологічної революції: технологічні зміни; розробка систем; операційні інновації; організаційна адаптація [20].

Одним із найважливіших компонентів системи соціальних інформаційно-психологічних відносин сучасного суспільства є інформаційно-психологічний конфлікт – основна форма взаємодії суб'єктів соціальної діяльності, що дає змогу своєчасно виявляти й усувати виникаючі в цих відносинах суперечності. Інформаційно-психологічна війна – найбільш яскравий приклад гострого інформаційно-психологічного конфлікту, що характеризується високим ступенем інтенсивності, агресивності та соціальної небезпеки [21].

Незважаючи на розмаїття форм і методів ведення інформаційно-психологічної війни, що розробляються та використовуються учасниками інформаційного протиборства в цей час, інформаційно-психологічна війна, як і раніше, залишається одним із різновидів соціального конфлікту, закономірності виникнення, розвитку та згасання якого визначаються психологією людських відносин, що практично не змінилася, якщо вірити антропологам, з появи людини розумної [22].

Однією з найважливіших дослідницьких завдань соціальної конфліктології інформаційного суспільства, безсумнівно, є формування системи поглядів на генезу інформаційно-психологічного конфлікту, що визначає закономірності зародження та розвитку конфліктів в інформаційній (інформаційно-психологічній) сфері, їх видову трансформацію, появу найбільш небезпечних агресивних форм у результаті послідовної еволюції низки стандартних і передбачуваних у рамках положень цієї теорії конфліктних ситуацій, які можна визначити як стадії розвитку конфлікту [23].

Розглядаючи інформаційно-психологічну війну в широкому розумінні як цілеспрямоване та планомірне використання політичними опонентами інструментів інформаційно-психологічного впливу й інших засобів (дипломатичних, військових, економічних, політичних тощо) для прямого чи непрямого впливу на думки, настрої, почуття та, як результат – на поведінку противника, щоб змусити його діяти в угодних напрямах, можна говорити про те, що, як компонент системи політичних відносин, інформаційно-психологічна війна присутня в різних вимірах цієї системи не лише як зовнішня, але і як внутрішня політика [24].

У відповідь на інформаційну агресію з боку російської федерації, у 2017 р. указом Президента України введено в дію Доктрину інформаційної безпеки. Метою Доктрини є уточнення засад формування й реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу російської федерації в умовах розв'язаної нею гібридної війни. Доктрина ґрунтується на принципах додержання прав і свобод людини й громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету й територіальної цілісності України [25].

Отже, виокремлення інформаційно-психологічної безпеки особистості із загальної проблематики інформаційної безпеки як самостійного напряму визначається такими основними причинами. Першою постає перехід до інформаційного суспільства, збільшення масштабів та ускладнення змісту й структури інформаційних потоків, які значно посилюють їх вплив на психічний стан людини. Це визначає необхідність формування нових механізмів і засобів виживання людини як особистості й активного соціального суб'єкта в сучасному світі.

Другою причиною є взаємодія психіки людини з інформаційним середовищем, яка відрізняється своєю специфікою та не має адекватних аналогів в інформаційній взаємодії інших біологічних, технічних, соціальних і соціотехнічних систем [26].

Також потрібно зауважити, що основною «мішенню» інформаційного впливу є людина, її психічний стан. Саме з окремих особистостей, їх взаємодії залежить нормальне функціонування соціальних суб'єктів різного рівня складності, будь-яких спільнот і соціальних груп від малої групи до населення країни в цілому.

Загальним джерелом зовнішніх загроз інформаційно-психологічної безпеки особистості є та частина інформаційного середовища суспільства, яка через різні причини неадекватно відображає навколишній світ. Тобто інформація, яка вводить людей в оману, у світ ілюзій, не дає змоги реально сприймати світ і себе в ньому.

За деякими прогнозами, швидке вдосконалення методів цілеспрямованого впливу на інформаційні та психологічні процеси в системах державного управління «противника» спроможні не лише вплинути на стратегічний баланс сил, що склався у світі, але й змінити самі нині відомі критерії оцінки такого балансу на основі співвідношення геополітичних, економічних і військових чинників [27].

Тенденції, що спостерігаються в останні роки, у розвитку інформаційних технологій можуть уже в недалекому майбутньому призвести до появи якісно нових (інформаційних) форм боротьби, у тому числі й на міждержавному рівні, які можуть набувати форми так званої інформаційної війни, а сама інформаційна війна стане одними з основних. інструментів зовнішньої політики, уключаючи захист державних інтересів та реалізацію будь-яких форм агресії.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Подальший прогрес людства однозначно пов'язано із широким упровадженням інформаційно-комунікаційних технологій або, іншими словами, із побудовою інформаційного суспільства. Його розвиток, висока динаміка збільшення кількості суспільних відносин, що ґрунтуються на широкому використанні інформації й інформаційних процесів, різке підвищення значущості цих відносин для всіх сфер життєдіяльності людини, суспільства та держави обумовлюють актуальність і необхідність вивчення теоретичних, методологічних та практичних проблем правового забезпечення інформаційної сфери, основою якого є інформаційне право й інформаційне законодавство.

Поряд із юридичними конструкціями, правилами та прийомами викладення законодавчих й інших нормативно-правових актів чи не найважливішим засобом юридичної техніки є відповідна термінологія.

Система визначень, що характеризує різні аспекти інформаційної діяльності, стає основою формування відповідних безпекових понять, необхідних для розвитку технологій організації та забезпечення інформаційної безпеки. А втім, термінологія, що застосовується у сфері забезпечення інформаційної безпеки, демонструє на брак єдності, неоднозначні тлумачення, а то й узагалі відсутні визначення багатьох понять, у тому числі ключових. Усе це створює серйозні перешкоди як для правотворчої діяльності в інформаційній сфері, так і для правозастосовної, а також зайвий раз засвідчує відсутність системності в розв'язанні вказаних проблем.

Наприклад, до теперішнього часу немає законодавчого визначення такого базового терміна, як «безпека інформації», хоча таке термінологічне сполучення вживається в деяких законах. У Законі України «Про основи національної безпеки», який був основним орієнтиром забезпечення безпеки України, системна сутність безпеки інформації трактувалася як невід'ємна складова частина національної безпеки України, не даючи при цьому її точного визначення. Крім того, у цьому Законі, замість поняття «інформаційна безпека України», використовувався термін «національна безпека України в інформаційній сфері». Визначення поняття «інформаційна безпека», різні за своєю суттю й у Законах України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та «Про телекомунікації». У більшості наукових праць із питань інформаційної безпеки здебільшого розглядаються суто технічні питання захисту інформації: захист інформаційно-телекомунікаційних систем, каналів передачі інформації, доступ до інформації, розробка засобів захисту баз даних, захист від витоку інформації тощо.

У Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «інформаційна безпека» визначається як стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається нанесення шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання та порушення цілісності, конфіденційності й доступності інформації. Проте потрібно враховувати, що цей правовий акт розроблявся і був прийнятий до початку явних проявів гібридної війни.

На думку О. Довгань та Т. Ткачук, визначено інформаційну безпеку України як стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури,

інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб'єктів, а також досягнення відповідних національних цілей і реалізація національних інтересів в інформаційній сфері. При цьому забезпечення інформаційної безпеки держави – це постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й спроможні контролюватися тривалий час [28].

Однією з ключових частин Військово-технологічної революції у сучасному світі є можливість розвитку нової форми ведення війни, яку часто називають інформаційною. Розвиток інформаційної війни залежить від технологічних змін, розвитку систем та адаптації оперативних підходів й організаційних структур, щоб скористатися цією новою можливістю. У військовій галузі велику увагу по праву зосереджено на оцінці доктринальних, оперативних та організаційних питань революції в галузі інформаційної війни. Але набагато менше уваги приділяється конкретному впливу інформаційної війни на технологічні дослідження та придбання [29].

Загрози інформаційних воєн, спекулятивних (ворожих, агресивних) інформаційних впливів нагально ставлять питання інформаційної безпеки. Законодавець визначив основні загрози інформаційній безпеці, зважаючи на динамічність і радикальність можливих змін, а також завдяки інтенсивному науково-технічному прогресу. Тому будь-який закон навряд чи зможе або має містити вичерпний перелік таких загроз задля відображення сучасних проблем. Вважається суттєвим недоліком у законі відсутність такої загрози як обмеження реалізації прав та свобод людини й громадянина щодо використання, поширення та зберігання інформації [30].

Озброївшись припущенням, що основна частина технологій інформаційної війни надходитиме з комерційного сектору, ми повинні з'ясувати, що мусить робити централізована система військових досліджень. Здається очевидним, що все ще існує роль у світі придбань, хоча вона може дещо відрізнятися від сучасної. По-перше, він повинен визначити ті сфери, де діловий світ не може відповідати військовим потребам. Це той самий вид діяльності, який уже виконувався для інших технологій, корисних для військових. Наприклад, багато аерокосмічних технологій, які використовуються військовими, широко доступні в комерційних аерокосмічних компаніях. Але такі предмети, як катапульти та ракетні установки, не є стандартним комерційним тарифом, і тому військові повинні забезпечити фінансовий поштовх для розробки й придбання такої

продукції. Те саме стосується унікальних військових технологій, корисних для інформаційної війни [31].

По-друге, потрібно продовжувати тенденцію до децентралізації закупівель інформаційних технологій. Завдяки розробці комерційних стандартів, що сприяють сумісності та впровадженню технологій, можливо, що кваліфіковані місцеві користувачі зможуть швидко закуповувати й будувати системи для кращого задоволення власних потреб. Спільнота поглиначів не повинна боротися з цією тенденцією, намагаючись утримати контроль над стандартами, тим більше, що дані про операційну сумісність попередніх централізованих систем були менш вражаючими. Відвертаючись від загальних тем інформаційних технологій, бачимо, що існує конкретна проблема захисту інформації під час придбання й розробки систем. Оскільки залежність від комерційних технологій породжує супутню вразливість до комерційних технологій, важливо оцінити ризики, що їх створюють ці вразливості «заздалегідь і на початку» в циклі розробки [32].

Уже існують методології для проведення таких оцінок як частина інженерного процесу – і ці методології треба посилити та розширити їх використання до всіх нових або модифікованих систем. Крім того, треба вирішити занепокоєння щодо цілісності продукту через «бекдори» програмного забезпечення. Оскільки ці проблеми цікавлять і комерційні структури, військові повинні прагнути набагато тісніше взаємодіяти з традиційно не оборонними фірмами, які надають значну частину відомостей для військової інформаційної інфраструктури задля розв'язання цих проблем.

Сподіваємося, що вітчизняні законодавство й програмні продукти у сфері забезпечення інформаційної безпеки матимуть новий сучасний зміст, що відповідатиме високому світовому рівню.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Голови Служби безпеки України від 10.08.2021 р. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 04.07.2020 р. № 31 ст. 286

3. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. URL: www.president.gov.ua /dokument/17588.html.

4. Про інформацію: Закон України від 2 жовтня 1992 р. *Відомості Верховної Ради України*, 1992, № 48, ст. 650.

5. Президент затвердив Положення про Центр протидії дезінформації. URL: https://www.president.gov.ua/news/prezident-zatverdiv-polozhennya-pro-centr-protidiyi-dezinfor-68317

6. Про основи національної безпеки України: Закон України від 19 черв. 2003 р. № 964-IV, 2003, № 9. ст. 351. URL https://zakon.rada.gov.ua/laws/show/964-15#Text

7. Про Службу безпеки України: Закон України від 25.03.1992 № 2229–XII. *Відомості Верховної Ради України*, 1992, № 27, ст. 382. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

8. Про Національну поліцію: Закон України від 08.08.2021р. № 580-VIII. *Відомості Верховної Ради України*, 2015, № 40–41, ст. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

9. Про стратегію національної безпеки України: Указ Президента України від 12.02.2007 р. *Урядовий кур'єр*, 2007, 7 берез. URL: https://zakon.rada.gov.ua/laws/show/105/2007#Text

10. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України. *Урядовий кур'єр*, 2007, 14 лют.

11. Курбан, О. В. (2016). Сучасні інформаційні війни в мережевому онлайн просторі: навч. посіб. Київ: ВІКНУ, 286 с. URL: http://www.mil.univ.kiev.ua/files/222_1044284240.pdf.

12. Гарасимчук, О. І. (2010). Комплексні системи санкціонованого доступу: навч. посіб. Львів: Вид. Львів. політехніки, 212 с.

13. Валюшко, І. О. (2015). Еволюція інформаційних війн: минуле і сучасність. *Історико-політичні студії*, № 2, с. 127–134. URL: https://ir.kneu.edu.ua/bitstream/handle/2010/17471/127-134.pdf?sequence=1&isAllowed=y

14. Прибутько, П. С. (2007). Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: вид., 252 с.

15. Бегма, В. М. (2011). Військово-технічне співробітництво в умовах глобалізації: український вимір. Київ: НІСД, с. 80. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

16. Прибутько, П. С. (2007). Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: вид., 252 с.

17. Горбулін, В. П. (2008). Актуальні проблеми системного забезпечення інформаційної безпеки України. *Форми та методи забезпечення інформаційної безпеки держави*: матеріали міжнар. наук.-практ. конф. «Форми та методи забезпечення інформаційної безпеки держави» (Київ, травень, 20008 р.). Київ: Нац. Акад. СБ України, с. 79–85.

18. Бегма, В. М. (2011). Військово-технічне співробітництво в умовах глобалізації: український вимір. Київ: НІСД, с. 80. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

19. Кириленко, І. В. Основи оборонної економіки. URL: https://mil.univ.kiev.ua/files/63_1136594066.pdf

20. Бегма, В. М. (2011). Військово-технічне співробітництво в умовах глобалізації: український вимір. Київ: НІСД, с. 80. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

21. Кравченко, В. Ю. (2015). Теорія «гібридної війни»: український вимір. *Вісник Дніпропетровського університету: Фаховий журнал*, № 2. URL: http://repo.dma.dp.ua/897/1/.pdf

22. Макаренко, Л. П. Еволюція форм та методів ведення інформаційної війни. URL:http://oaji.net/articles/2014/797-1402908125.pdf

23. Макаренко, Л. П. Еволюція форм та методів ведення інформаційної війни. URL:http://oaji.net/articles/2014/797-1402908125.pdf

24. Почепцов, Г. (2017). Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ: ВД «Києво-Могилянська академія», 260 с.

25. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL :https://www.president.gov.ua/documents/472017–21374.

26. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукр. наук.практ. конф. (м. Маріуполь, 9 черв. 2017 р.). Маріуполь: ДонДУУ, 2017, 311 с. URL: https://www.google.com.ua.

27. Кравченко, В. Ю. (2015). Теорія «гібридної війни»: український вимір. *Вісник Дніпропетровського університету: фаховий журн*., № 2. URL: http://repo.dma.dp.ua/897/1/.pdf

28. Довгань, О., Ткачук, Т. (2019). Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*, № 1, с. 86–99. URL: http://nbuv.gov.ua/UJRN/Infpr_2019_1_12

29. Бегма, В. М. (2011). Військово-технічне співробітництво в умовах глобалізації: український вимір. Київ: НІСД, 80 с. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

30. Росія витрачає на війну в Україні бюджети цілих країн. ІНФОГРАФІКА. URL: http://www.volynpost.com/news/61241-rosiia-vytrachaie-na-vijnu-v-ukraini-byudzhety-cilyh-krain-infografika

31. Курбан, О. В. (2016). Сучасні інформаційні війни в мережевому онлайн просторі: навч. посіб., Київ: ВІКНУ, 286 с. URL: http://www.mil.univ.kiev.ua/files/222_1044284240.pdf.

32. Гарасимчук, О. І. (2010). Комплексні системи санкціонованого доступу: навч. посіб. Львів: Видавництво Львівської політехніки, 212 с.

REFERENCES

1. Pro zatverdzhennia Zvodu vidomostei, shcho stanovliat derzhavnu taiemnytsiu: nakaz Holovy Sluzhby bezpeky Ukrainy vid 10.08.2021 r. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text

2. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh: Zakon Ukrainy vid 04.07.2020 r. № 31 st.286

3. Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 r. URL: www.president.gov.ua / dokument/17588.html.

4. Pro informatsiiu: Zakon Ukrainy vid 2 zhovtnia 1992 r. Vidomosti Verkhovnoi Rady Ukrainy, 1992, № 48, st. 650.

5. Prezydent zatverdyv Polozhennia pro Tsentr protydii dezinformatsii. URL: https://www.president.gov.ua/news/prezident-zatverdiv-polozhennya-pro-centr-protidiyi-dezinfor-68317

6. Pro osnovy natsionalnoi bezpeky Ukrainy: Zakon Ukrainy vid 19 cherv. 2003 r. № 964-IV, 2003, № 9, st. 351. URL https://zakon.rada.gov.ua/laws/show/964-15#Text

7. Pro Sluzhbu bezpeky Ukrainy: Zakon Ukrainy vid 25.03.1992 № 2229–XII. Vidomosti Verkhovnoi Rady Ukrainy, 1992, № 27, st. 382. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

8. Pro Natsionalnu politsiiu: Zakon Ukrainy vid 08.08.2021 r. № 580-VIII. Vidomosti Verkhovnoi Rady Ukrainy, 2015, № 40–41, st. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

9. Pro stratehiiu natsionalnoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 12.02.2007 r. Uriadovyi kurier, 2007, 7 berez. URL: https://zakon.rada.gov.ua/laws/show/105/2007#Text

10. Pro osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky: Zakon Ukrainy. Uriadovyi kurier, 2007, 14 liut.

11. Kurban, O. V. (2016). Suchasni informatsiini viiny v merezhevomu on-lain prostori: navch. posib. Kyiv: VIKNU, 286 s. URL: http://www.mil.univ.kiev.ua/files/222_1044284240.pdf.

12. Harasymchuk, O. I. (2010). Kompleksni systemy sanktsionovanoho dostupu: navch. posib. Lviv: Vyd. Lviv. politekhniky, 212 p.

13. Valiushko, I. O. (2015). Evoliutsiia informatsiinykh viin: mynule i suchasnist. Istoryko-politychni studii, № 2, p. 127–134. URL: https://ir.kneu.edu.ua/bitstream/handle/2010/17471/127-134.pdf?sequence=1&isAllowed=y

14. Prybutko, P. S. (2007). Informatsiini vplyvy: rol u suspilstvi ta suchasnykh voiennykh konfliktakh. Kyiv: vyd., 252 p.

15. Behma, V. M. (2011). Viiskovo-tekhnichne spivrobitnytstvo v umovakh hlobalizatsii: ukrainskyi vymir. Kyiv: NISD, p. 80. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

16. Prybutko, P. S. (2007). Informatsiini vplyvy: rol u suspilstvi ta suchasnykh voiennykh konfliktakh. Kyiv: vyd., 252 p.

17. Horbulin, V. P. (2008). Aktualni problemy systemnoho zabezpechennia informatsiinoi bezpeky Ukrainy. Formy ta metody zabezpechennia informatsiinoi bezpeky derzhavy: materialy mizhnar. nauk.-prakt. konf. «Formy ta metody zabezpechennia informatsiinoi bezpeky derzhavy» (Kyiv, traven, 20008 r.). Kyiv: Nats. Akad. SB Ukrainy, p. 79–85.

18. Behma, V. M. (2011). Viiskovo-tekhnichne spivrobitnytstvo v umovakh hlobalizatsii: ukrainskyi vymir. Kyiv: NISD, s. 80. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

19. Kyrylenko, I. V. Osnovy oboronnoi ekonomiky. URL: https://mil.univ.kiev.ua/files/63_1136594066.pdf

20. Behma, V. M. (2011). Viiskovo-tekhnichne spivrobitnytstvo v umovakh hlobalizatsii: ukrainskyi vymir. Kyiv: NISD, p. 80. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

21. Kravchenko, V. Yu. (2015). Teoriia «hibrydnoi viiny»: ukrainskyi vymir. Visnyk Dnipropetrovskoho universytetu: Fakhovyi zhurnal, № 2. URL: http://repo.dma.dp.ua/897/1/.pdf

22. Makarenko, L. P. Evoliutsiia form ta metodiv vedennia informatsiinoi viiny. URL:http://oaji.net/articles/2014/797-1402908125.pdf

23. Makarenko, L. P. Evoliutsiia form ta metodiv vedennia informatsiinoi viiny. URL:http://oaji.net/articles/2014/797-1402908125.pdf

24. Pocheptsov, H. (2017). Vid pokemoniv do hibrydnykh viin: novi komunikatyvni tekhnolohii XXI stolittia. Kyiv: VD «Kyievo-Mohylianska akademiia», 260 p.

25. Ukaz Prezydenta Ukrainy №47/2017 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy». URL :https://www.president.gov.ua/documents/472017–21374.

26. Ukrainske suspilstvo v umovakh viiny: vyklyky sohodennia ta perspektyvy myrotvorennia: materialy Vseukr. nauk.prakt. konf. (m. Mariupol, 9 cherv. 2017 r.). Mariupol: DonDUU, 2017, 311 p. URL: https://www.google.com.ua.

27. Kravchenko, V. Yu. (2015). Teoriia «hibrydnoi viiny»: ukrainskyi vymir. Visnyk Dnipropetrovskoho universytetu: fakhovyi zhurn., № 2. URL: http://repo.dma.dp.ua/897/1/.pdf

28. Dovhan, O., Tkachuk T. Kontseptualni zasady zakonodavchoho zabezpechennia informatsiinoi bezpeky Ukrainy. Informatsiia i pravo. 2019. № 1, p. 86–99. URL: http://nbuv.gov.ua/UJRN/Infpr_2019_1_12

29. Behma, V. M. (2011). Viiskovo-tekhnichne spivrobitnytstvo v umovakh hlobalizatsii: ukrainskyi vymir. Kyiv: NISD, 80 p. URL: https://niss.gov.ua/sites/default/files/2011-10/vtc-e8633.pdf

30. Rosiia vytrachaie na viinu v Ukraini biudzhety tsilykh krain. INFOHRAFIKA URL: http://www.volynpost.com/news/61241-rosiia-vytrachaie-na-vijnu-v-ukraini-byudzhety-cilyh-krain-infografika

31. Kurban, O. V. (2016). Suchasni informatsiini viiny v merezhevomu on-lain prostori: navch. posib., Kyiv: VIKNU, 286 p. URL: http://www.mil.univ.kiev.ua/files/222_1044284240.pdf.

32. Harasymchuk, O. I. (2010). Kompleksni systemy sanktsionovanoho dostupu: navch. posib. Lviv: Vydavnytstvo Lvivskoi politekhniky, 212 p.

Матеріал надійшов до редакції 05.09.2022 р.