© Tkach Yu. Trends in the development of modern cyber space and its security in conditions of information conflict // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 74-79.

DOI: 10.18372/2225-5036.26.14916

ТЕНДЕНЦІЇ РОЗВИТКУ СУЧАСНОГО КІБЕРПРОСТОРУ ТА ЙОГО ЗАХИЩЕНОСТІ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Юлія Ткач

Національний університет «Чернігівська політехніка»

ТКАЧ Юлія Миколаївна, д.пед.н., доцент

Рік та місце народження: 1979 рік, м. Чернігів, Україна.
Освіта: Чернігівський національний технологічний університет, 2012 рік; Чернігівський державний педагогічний університет ім. Т.Г. Шевченка, 2001.
Посада: завідувач кафедри кібербезпеки та математичного моделювання з 2010 р.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 80 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: tkachym79@gmail.com.
Orcid ID: 0000-0002-8565-0525.

Анотація. *У статті розглянуто актуальне питання формування кіберпростору та особливості його захисту. Визначено тенденції його розвитку в умовах інформаційного протиборства, а саме: інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі; кіберпростір поступово перетворюється у п'ятий театр військових дій; для забезпечення переваги у кіберпросторі провідні країни світу починають формувати військово-мережевий комплекс; проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації; надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу. Зроблено висновок, що в умовах, що сьогодні склались, тобто інформаційного протиборства, принципове значення має підтримка розробки і виробництва в Україні конкурентних інформаційно-комунікаційних засобів (у тому числі, з використанням вітчизняної мікроелектроніки, яку потрібно відновити та розвивати) та програмного забезпечення в інтересах українських користувачів, а також застосування таких засобів в Україні, і передусім, в оборонному комплексі і на об'єктах критичної цивільної інфраструктури, з метою протидії інформаційним впливам.*

Ключові слова: *інформаційне протиборство, інформаційний простір, кіберпростір, кібербезпека, інформаційна безпека.*

Актуальність

Стрімкий розвиток інформаційних технологій, надзвичайно висока активність засобів масових інформації в житті суспільства обумовили масштабні інформаційні впливи як на окрему людину, так і на цілі країни. Це в свою чергу спричинило появу нових технічних й психологічних засобів, які здатні впливати на психіку та свідомість окремої особистості й цілих націй. Таким чином, розпочалась ера інформаційного протиборства.

Аналіз останніх досліджень

У сучасній літературі проблема інформаційного протиборства розглядалась багатьма науковцями, зокрема Т. Батура, Горбулін В., Грищук Р., Р. Гумінський, Додонов О., Князєва Є., Д. Ланде, Молодецька К., Новиков Д., Почепцов Г., Пую А. , Розторгуєв С., Б. Хоган, Хорошко В., Чхартишвили А. та ін. Незважаючи на це, актуальними та малодослідженими залишись питання формування кіберпростору та визначення тенденцій його розвитку в сучасних умовах та врахування при цьому стану інформаційного протиборства.

Виділення невирішених раніше частин загальної проблеми

Незважаючи на численні дослідження у напрямку захисту інформації, досі залишаються не визначеними тенденції розвитку захищеного кіберпростору, особливо важливо це зробити в сучасних умовах інформаційного протиборства

Метою статті є визначення тенденції розвитку сучасного кіберпростору та особливостей його захищеності в умовах інформаційного протиборства.

Виклад основного матеріалу

В умовах інформаційного протиборства розвиток бездротових технологій та цифрової інфраструктури радикально змінило відношення людини зі своїм середовищем проживання та друг з другом. Інтернет-технології глибоко проникли у різні сфери життєдіяльності, повсякденними стали елементи електронного світу (електронний уряд, електронні пос-

луги, електронні документи, електронні гроші, електронний підпис), звичайним стало дистанційне навчання, наради, робота тощо. Тобто сформувалась нова сутність ***кіберпростір*** (cyberspace). Кіберпростір став середовищем для маніпулювання суспільною думкою і тим самим став джерелом інформаційно-психологічних впливів. При цьому, засоби, що використовуються є досить різноманітними, від технічних до психологічних.

Розглянемо як на даний час співвідносяться між собою поняття інформаційний простір, кіберпростір та кібербезпека.

Інформаційний простір (рис. 1) – це область ведення інформаційної війни, дії в якому можуть розгортатися як в психологічній сфері, так і в технічній сфері [11].

Психологічна сфера - це область інформаційного простору, яка об'єднує мислення особового складу ЗС та мирного населення. Це область, в якій формуються наміри командирів, доктрини, тактика, методи протиборства, мораль, поняття згуртованості підрозділів, рівень підготовки, досвід, розуміння ситуації та суспільна думка населення [12].

Технічна сфера - це область інформаційного простору, в якій створюється, обробляється та накопичується інформація. Крім того, це область, в якій функціонують системи управління, зв'язку та розвідки [12]. В подальшому в ряді керівних документів розвиток та уточнення поняття технічної сфери інформаційного простору призвело до створення понятійного апарату кіберпростору.

Вперше загальне визначення кіберпростору було надано дослідницькою службою конгресу США для того, щоб через термінологічний базис "кіберпонять" визначати сутності, які відносяться до протиборства в технічній сфері інформаційного простору (іншими словами, області ведення інформаційної війни) [1-2]. Основи цієї термінології надані в керівних документах ЗС США [3-7] та міжнародних стандартах ITU-T та ISO [8-10].

Рис. 1. Декомпозиція інформаційного простору [12]

Кіберпростір - всеохоплююча множина зв'язків між людьми, яка створена на основі комп'ютерів та телекомунікацій незалежно від фізичного чи географічного положення [5].

У Єдиному статуті комітету начальників штабів Збройних сил США кіберпростір визначено наступним чином [5]: «*Кіберпростір* - це сфера (область), в якій застосовуються різні РЕЗ (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління та наведення) для прийому, передачі, обробки, зберігання, трансформації інформації та пов'язана з ними інформаційна інфраструктура ЗС».

У міжнародному стандарті ISO/IEC 27032:2012 [8] кіберпростір визначено з урахуванням тенденцій розвитку глобальної мережі Інтернету: *Кіберпростір* - це середовище, яке не існує у будь-якій фізичній формі, та являє собою наслідок результату взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомоги технологій, засобів та мереж. У цьому ж стандарті через поняття кіберпростір визначено також термін "кібербезпека": *Кібербезпека* - це безпека в кіберпросторі [8].

У рекомендації X.1205 МСЭ-Т [9] кібербезпека визначена через поняття кіберпростору та систему управління ризиками: *Кібербезпека* — це набір засобів, стратегій, принципів забезпечення безпеки, мір з забезпечення безпеки, керівних принципів, підходів к керівництву ризиками, дій, професійної підготовки, практичному досвіду, страхуванню та технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача.

Стандарт ISO/IEC 27032:2012 [8] визначає зв'язок термінів кібербезпека, мережева безпека, прикладна безпека, Інтернет безпека та безпека критичних інформаційних інфраструктур. В стандарті надана візуалізація зв'язку цих термінів (рис. 2). З точки зору міжнародних експертів усі ці терміни об'єднує поняття інформаційна безпека.

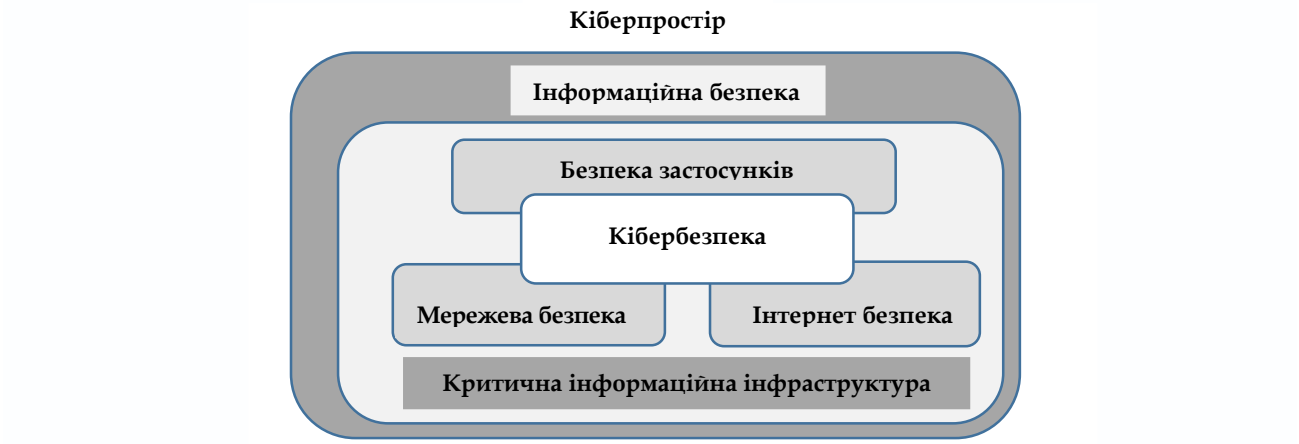

Рис. 2. Зв'язок терміну «кібербезпека» с термінологічним базисом стандарту ISO/IEC 27032:2012 [8]

Таким чином, основу кіберпростору складають сукупність розподілених у просторі взаємопов'язаних електронних засобів (комп'ютерів, серверів, мережевих маршрутизаторів, сховищ даних, шифраторів тощо) з відповідним програмним забезпеченням, за допомогою яких створюється та циркулює інформація (обробляється, передається, запам'ятовується та зберігається).

С інфраструктурної точки зору глобальний кіберпростір можна розглядати як адресний простір, що складається з національних та регіональних сегментів Інтернету.

Суб'єктами кіберпростору є людина, суспільство, держава, а також жива істота, яка спроможна сприйняти, запам'ятати та переробити інформацію, а також обмінятися нею [19].

Аналізуючи процес розвитку кіберпростору можна виділити декілька цікавих тенденцій, які в найближчому майбутньому суттєво вплинуть на його функціювання.

Тенденція перша: *Інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі.*

Фактор наявності кіберпростору починає істотно впливати на інформаційну сферу будь-якої держави. З точки зору інтересів країни, кіберпростір треба розглядати як частину національної інфраструктури, яка має окреслені межі та потребує певної системи безпеки, як й інші елементи державної інфраструктури. Основна проблема кіберпростору - це забезпечення безпеки інформації, яка там циркулює, та стійкість його національного сегменту к кібератакам.

Інформаційна зброя стирає відмінність між військовими цілями і цивільними об'єктами, що обумовлено тісним взаємозв'язком та взаємозалежністю військових і цивільних інформаційних інфраструктур. Можна припустити, що в майбутньому високотехнологічні цивільні інформаційні системи, у тому числі що підтримують роботу критичних інфраструктур, будуть головними цілями нападу зі сторони можливого противника.

Перемога у інформаційному протиборстві в кіберпросторі може вирішити остаточний результат військового протиборства в цілому і вона може бути досягнута без здійснення традиційних бойових операцій, а тільки за рахунок застосування інформаційно-комунікаційні технології.

Тенденція друга: *кіберпростір поступово перетворюється у п'ятий театр військових дій.*

Кіберпростір поряд з традиційними наземним, морським, повітряним та космічним стає новим театром військових дій, де разом з військами планується участь спецслужб країни, хакерів та усіх тих, хто може створювати та використовувати інформаційні технології для нанесення ударів по ворогу.

Ряд країн (в першу чергу, США, Росія, Китай) вже проводять державну політику, яка розглядає кіберпростір як поле боя, внаслідок чого направляє свої зусилля на встановлення повного контролю в цій сфері, створюючи засоби та можливості на здійснення такого контролю. Такі прецеденти численні - інформаційна зброя використовувалася в усіх військових конфліктах на протязі останніх двадцяти років, вона стала важливою частиною озброєння збройних Китаю, Росії, США та їх союзників. Є дані, що роботи щодо розвитку потенціалу інформаційного протиборства проводять більш ніж 120 країн світу (для прикладу, розробки в області ядерної зброї ведуть не більше 20 країн).

Війни майбутнього будуть вестися в режимі онлайн, коли противник, окрім застосування сил на полі бою, буде використовувати вразливості комп'ютерних систем озброєння, інформаційних систем керування державних структур та об'єктів критичної інфраструктури для їх руйнування та знищення, а також соціальні мережі для створення паніки серед населення в масштабі цілої країни для зниження його здатності к супротиву агресії.

Кібервійни з фантастичних романів перекочовують у реальність. Вже відбувається трансформація усієї військової інформаційної архітектури, спостерігається "інформатизація" традиційних збройних сил і "інтелектуалізація" озброєнь. Активно розвивається концепція ексцентричного ведення бойових дій, мається на увазі досягнення переваги над ворогом шляхом ефективної організації збору, обробки і використання інформації.

Сьогодні можна вже говорити про те, що інформаційна зброя в деяких розвинених країнах перей-

шла в розряд тактичної. Повідомляється про розробки високочастотної електромагнітної імпульсної зброї, здатної виводити з ладу електроніку в радіусі сотень кілометрів. Експерти відмічають, що низка країн такі можливості має в розпорядженні вже нині. Ведуться розробки мікрохвильової зброї великої потужності, здатної змінювати траєкторію ракет у польоті, викликати перевантаження або виведення із ладу мереж зв'язку, телеметричного устаткування та електроніки систем озброєння. Вона також здатна вражати екрановані приміщення, захищені від радіоактивного випромінювання, та завдавати збитку здоров'ю й життю осіб, що знаходяться в радіусі її дії.

Тенденція третя: *для забезпечення переваги у кіберпросторі провідні країни світу починають формувати військово-мережевий комплекс.*

В часи "холодної війни", коли за відсутності активних воєнних дій розгорнулася безпрецедентна "гонка озброєнь", в США та СРСР уперше виникли так звані військово-промислові комплекси (ВПК). Основною задачею ВПК на першому плані виступив такий чинник могутності, як спроможність розробляти й виготовляти озброєння та військову техніку (ОВТ) на сучасному рівні і в належній кількості.

Під військово-промисловим комплексом розуміють сукупність підприємств і організацій тієї чи іншої країни, що виготовляють ОВТ для потреб збройних сил своєї держави та на експорт (рис.3). В офіційних документах України (а також Росії) зараз замість ВПК, як правило, вживається термін оборонно-промисловий комплекс [13].

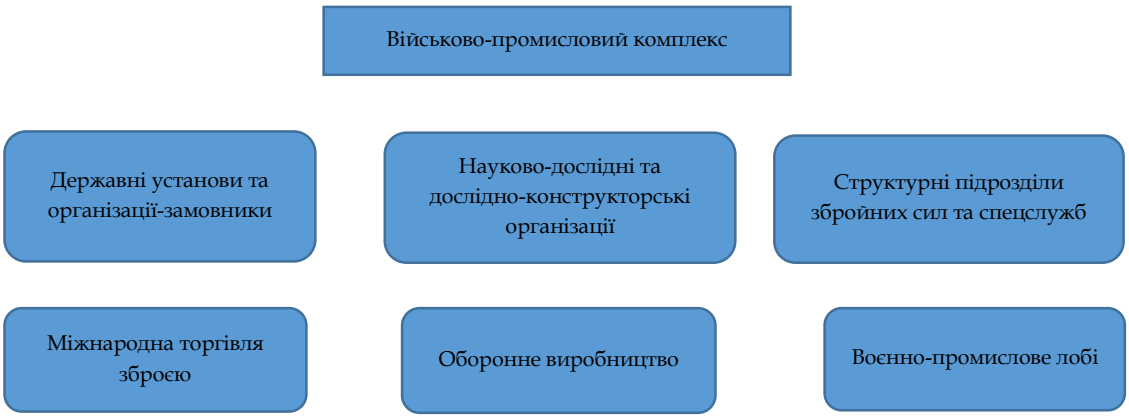

Рис. 3. Структура військово-промислового комплексу

Військово-промисловий комплекс – це суспільний феномен, у підґрунті якого лежить збіг інтересів керівництва воєнних корпорацій, вищого командного складу ЗС і високих посадових осіб держави, а одним з головних проявів є лобіювання бізнес-інтересів воєнної промисловості на вищому державному рівні та посилення її впливу на суспільні процеси. До нього звичайно зараховують ракетно-космічну, авіабудівну, суднобудівну, бронетанкову, радіоелектронну та артилерійсько-стрілецьку галузі.

Процеси, які зараз проходять в сфері інформаційного протиборства та кіберпростору, подібні процесам часів створення ВПК. Ми є свідками формування *військово-мережевого комплексу*, коли інтереси та можливості спецслужб і воєнного сектору країни переплітаються з інтересами та можливостями приватних структур, що в найближчий час разюче змінює як сам кіберпростір, так і характер воєнних дій в ньому.

Для вирішення цієї задачі відбувається колаборація державних структур з техноіндустрією Інтернету - крупними виробниками мікроелектроніки, обчислювальної та телекомунікаційної техніки щодо збору інформації о користувачах. В засобах масової інформації неодноразово з'являлися дані щодо співпраці зі спецслужбами таких відомих потужних виробники засобів телекомунікації (Cisco, Huaway), шифраторів (Crypto AG, Omnisec, Mils Electronic), програмного забезпечення (Microsoft), соціальних мереж (Facebook, Вконтакте, Одноклассники), антивірусних систем (Касперский, McAfee), постачальників послуг електронної пошти, мережевих та Інтернет-гігантів (Google, Yahoo, AT&T, CenturyLink, Verizon). Така співпраця включає навіть вбудовування необхідних бекдорів та передачі спецслужбам таємні вразливості в апаратному та програмному забезпеченні, у тому числі діючі ключі шифрування [15].

Тенденція четверта: *проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації.*

Існуючі проблеми інформаційної безпеки кіберпростору показують, що державні органи не будуть основними гравцями в цій сфері, усякому разі її постійними лідерами. Вони будуть виробляти стратегію, встановлювати закони і контролювати стандарти безпеки кіберпростору, а ключові об'єкти інфраструктури повинні будуть їх виконувати. Але повсякденна робота по захисту ключових промислових об'єктів стане турботою корпорацій, які впораються з цією задачею не гірше держави. Вони будуть створювати новий вид послуг зі сканування, аналізу трафіка та застосування власних методів виявлення шкідливих програм та хакерської активності - методів, які будуть основані на тих даних, які компанії будуть збирати в режимі реального часу в своїх інформаційних мережах, а також в мережах своїх клієнтів. Це виходить свого роду краудсорсінг, коли залучають до вирішення тих чи інших проблем інноваційної діяльності широке коло осіб для використання їх творчих здібностей, знань та досвіду для субпідрядної роботи із застосування інформаційних технологій.

Ці ж організації будуть створювати кіберармії та навчати їх воювати в мережі, що зрештою приведе до їх інтеграції з арсеналом збройних сил країни.

Тенденція п'ята: *Надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу.*

Більш того, ці ж самі організації будуть не просто розслідувати вже здійсненні вторгнення, а й пропонувати свої послуги по захисту мереж клієнтів від потенційних загроз, подібно тому, як охоронні фірми пропонують убезпечити наші дома і офіси від грабіжників.

Для того, щоб захиститись від повсякденних кіберзагроз будуть створюватися безпечні зони Інтернету, тобто повноцінні кібернетичні інфраструктури, у яких безпека буде поставлена на чільне місце, а трафік аналізуватися більш активно та ретельно, ніж у загальнодоступному Інтернеті. Це буде свого роду "екозона безпеки", онлайн аналог особливо охоронюваної території.

Підвищена кібербезпека стане привабливою споживчою якістю, той особливістю, яка буде залучати клієнтів. Кампанії, що візьмуться за створення та обслугу таких захищених кіберзон (інтернет-провайдери, банки та інші, що мають діло з персональними даними), будуть залучати найбільш досвідчених і кваліфікованих співробітників, оскільки рівень зарплат у них буде значно більший ніж у державному чи воєнному секторі.

Як і в любій приватній організації, власники такої інфраструктури зможуть обмежувати її користування, встановлювати правила й вимоги їх виконання, а також пропонувати особливі переваги, насамперед безпеку. В межах таких мереж буде ретельно проводитись аналіз трафіку щодо шкідливих програм, надсилатися попередження о потенційній загрозі особовим даним, проводиться контроль тих, хто намагається війти в мережу, та не допускати в неї будь-яких підозрілих користувачів.

Слід відзначити ще той факт, що у державному та військовому секторах багатьох країн використовуються комерційні програмні продукти, які майже завжди мають вади в захисті, робить обороноздатність країни потенційно уразливою для нападів кібернетичних сил противника (його військових формувань, спецслужб, хакерів та терористів).

Проблему інформаційної безпеки в Україні загострює фундаментальна залежність українських інформаційних інфраструктур від зарубіжних комп'ютерних засобів. Майже 90% об'ємів продажів телекомунікаційного устаткування на внутрішньому ринку (його місткість нараховується мільярдами доларів) припадає на зарубіжні устаткування, запасні частини або комплектуючі, що використовуються при ремонті та обслуговуванні. Така залежність небезпечна не лише з точки зору економічної безпеки країни, але й безпеки в ширшому контексті, особливо враховуючи, що зарубіжне програмне забезпечення широко використовується на стратегічних об'єктах українського оборонного комплексу. Відомі непоодинокі реальні прецеденти щодо закладок недокументованих програмних модулів для здійснення втручання в роботу програмного забезпечення.

Висновки. Таким чином, інформаційне протиборство в кіберпросторі буде являти собою комплекс заходів, які спрямовані на захист системи світоглядних орієнтирів, установок, стереотипів, на основі яких базується можливість особи або цілого народу дати відсіч агресору.

Виходячи з вищевикладеного, принципове значення має підтримка розробки і виробництва в Україні конкурентних інформаційно-комунікаційних засобів (у тому числі, з використанням вітчизняної мікроелектроніки, яку потрібно відновити та розвивати) та програмного забезпечення в інтересах українських користувачів, а також застосування таких засобів в Україні, і передусім, в оборонному комплексі і на об'єктах критичної цивільної інфраструктури, з метою протидії інформаційним впливам.

Література

[1]. *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington D.C.: The White House, 2009.

[2]. *Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* Washington D.C.: The White House, 2011.

[3]. *Department of Defense Strategy for Operating in Cyberspace*, Washington D.C.: U.S. Department of Defense, 2011.

[4]. *AFDD 3-12. Cyberspace Operations*, USAF, 2010, 60 p.

[5]. *AFDD 3-13. Information Operations*, USAF, 2011, 65 p.

[6]. *AFPD 10-7. Information Operations*, USAF, 2006, 29 p.

[7]. *DoDD 3600.1. Information Operations*, US DoD, 2013, 12 p.

[8]. *Стандарт ISO/IEC 27032:2012*. Інформаційні технології. Методи забезпечення безпеки. Керівні вказівки по забезпеченню кібербезпеки, 2012.

[9]. *Стандарт ITU-T X.1205:2008. Огляд кібербезпеки*, Женева: МСЭ-Т, 2008, 162 с. [Електронний ресурс]. Режим доступу: www.itu.int/ITU-T.

[10]. *Безпека в електрозв'язку та інформаційних технологіях. Огляд змісту та застосування діючих Рекомендацій МСЭ-Т для забезпечення захищеного електрозв'язку*, Женева: МСЭ-Т, 2009, 162 с. . [Електронний ресурс]. Режим доступу: www.itu.int/ITU-T.

[11]. *JP 3-13. Information Operations*, US Joint Chiefs of Staff, 2012, 69 p.

[12]. *JP 3-13.1. Electronic Warfare*, US Joint Chiefs of Staff, 2007, 115 p.

[13]. *Воєнно-промисловий комплекс* [Електронний ресурс]. Режим доступу: https://uk. wikipedia.org/wiki/ Воєнно-промисловий комплекс.

[14]. Я. Левин, *Интернет как оружие. Что скрывает Google, Tor и ЦРУ*, М.: Индивидуум, 2019, 360 с.

[15]. Ш. Харис, *Кибервойн@: Пятый театр военных действий,* М.: Альпина нон-фикшин, 2020, 390 с.

[16]. Л. Пирцхалава, В. Хорошко, Ю. Хохлачова, М. Шелест, *Информационное противоборство в современных условиях: [монография]*, Под ред. профессора В. Хорошко, К.: ЦП "Компринт", 2019, 226 с.

[17]. М. Карпінський, Ю. Ткач, Я. Усов, "Захищене інформаційне середовище", *ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р.*, К.: НАУ, С. 45-46, 2019.

[18]. Ю. Ткач, М. Шелест, М. Карпинський, "О развитии киберпространства и его защищенности", *I міжнародна науково-практична конференція «Безпека ресурсів інформаційних систем» (Information Systems of Security Resources), Чернігів, 16-17 квітня 2020 р.*,Чернігів, С. 103-105, 2020.

[19]. В. Фурашев, "Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності", *Інформація і право*, №2(5), С. 162-169, 2012.

УДК 004.056.5

Ткач Ю.Н. Тенденции развития современного киберпространстве и его защищенности в условиях информационного противоборства

Аннотация. *В статье рассмотрены актуальные вопросы формирования киберпространства. Определены тенденции его развития в условиях информационного противоборства, а именно: информационная безопасность напрямую зависит от кибербезопасности, есть политики безопасности, которая реализуется в киберпространстве; киберпространство постепенно превращается в пятый театр военных действий; для обеспечения преимущества в киберпространстве ведущие страны мира начинают формировать военно-сетевой комплекс; проблемы информационной безопасности в киберпространстве и формирования военно-сетевого комплекса приводят к перераспределению полномочий существующих игроков в сфере защиты информации; предоставление услуг по защите информации в киберпространстве становится новым видом бизнеса. Сделан вывод, что в условиях, сегодня сложились, то есть информационного противоборства, принципиальное значение имеет поддержка разработки и производства в Украине конкурентных информационно-коммуникационных средств (в том числе, с использованием отечественной микроэлектроники, которую нужно восстановить и развивать) и программного обеспечения в интересах украинских пользователей, а также применение таких средств в Украине, и прежде всего, в оборонном комплексе и на объектах критической гражданской инфраструктуры, с целью противодействия информационным воздействиям.*

Ключевые слова: *информационное противоборство, информационное пространство, киберпространство, кибербезопасность, информационная безопасность.*

Tkach Yu. Trends in the development of modern cyber space and its security in conditions of information conflict

Abstract. *The article considers the topical issue of cyberspace formation and features of its protection. It is proposed to distinguish between the concepts of information space, cyberspace and cybersecurity. Namely, the information space is an area of information warfare, actions in which can unfold both in the psychological sphere and in the technical sphere; cyberspace - a comprehensive set of connections between people, which is created on the basis of computers and telecommunications, regardless of physical or geographical location; Cybersecurity is a set of tools, strategies, security principles, security measures, guidelines, risk management approaches, actions, training, hands-on experience, insurance and technologies that can be used to protect cyberspace, organizational and user resources. The decomposition of the information space is determined and constructed. The tendencies of its development in the conditions of information confrontation are determined, namely: information security directly depends on cybersecurity, ie security policy implemented in cyberspace; cyberspace is gradually becoming the fifth theater of operations; to ensure the advantage in cyberspace, the world's leading countries are beginning to form a military-network complex; problems of information security in cyberspace and the formation of a military-network complex lead to a redistribution of powers of existing players in the field of information protection; the provision of information security services in cyberspace is becoming a new type of business. It is concluded that in the current conditions, ie information confrontation, it is essential to support the development and production in Ukraine of competitive information and communication tools (including the use of domestic microelectronics, which needs to be restored and developed) and software in the interests of Ukrainian users, as well as the use of such tools in Ukraine, and especially in the defense sector and at critical civilian infrastructure, in order to counter information influences.*

Keywords: *information confrontation, information space, cyberspace, cybersecurity, information security.*

Ткач Юлія Миколаївна, д.пед.н., доцент завідувач кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Ткач Юлия Николаевна, д.пед.н., доцент, заведующий кафедрой кибербезопасности и математического моделирования Национального университета «Черниговская политехника».

Tkach Yuliia, Doctor of Pedagogical Sciences, Associate Professor, Head of the Department of Cybersecurity and Mathematical Simulation of the National University "Chernihiv Polytechnic".

Отримано *02 липня 2020 року*, затверджено редколегією *29 липня 2020 року*