Руденко Оксана Ярославівна,
студентка IV курсу спеціальності «Документознавство та інформаційна діяльність», Національний університет «Острозька академія»

ІНТЕРНЕТ ЯК НОВЕ СЕРЕДОВИЩЕ ВЕДЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

У статті розкривається суть поняття «інформаційна війна», розглядаються її основні елементи, а також досліджується взаємозв'язок між інформаційним протиборством та Інтернетом. У статті представлені основні переваги використання Інтернету.

Ключові слова: *інформаційна війна, інформація, Інтернет, загроза, атака, небезпека.*

В статье раскрывается суть понятия «информационная война», рассматриваются ее основные элементы, а также исследуется взаимосвязь между информационным противоборством и Интернетом. В статье представлены основные преимущества использования Интернета.

Ключевые слова: *информационная война, информация, Интернет, угроза, атака, опасность.*

In this article the essence of concept «information warfare» is discovered, all its main components are considered. The interrelation between information contention and Internet is investigated. Fundamental advantages of Internet are presented in this paper.

Key words: *information warfare, information, Internet, threat, attack, danger.*

Із настанням XXI століття інформація посідає чи не найважливіше місце у житті людей. Звичайно, саме завдяки їй ми проходимо етап соціалізації, інтегруємося у суспільство. Завдяки інформації ми здобуваємо глибокі знання, отримуємо життєвий досвід, удосконалюємо власні здібності, покращуємо професійні навички, навчаємося чогось нового. Однак у зв'язку із науково-технічною революцією, розвитком новітніх технологій, прогресом засобів комунікації, впровадженням світових досягнень людства інформація розглядається абсолютно під іншим кутом зору. Тепер вона як ніколи є не лише основним регулятором і каталізатором будь-яких відносин, але і надпотужною зброєю та засобом впливу. Можна із впевненістю сказати, що сьогодні людство переживає глобальну інформатизацію, при чому залежність сучасного суспільства від якісної та релевантної інформації стрімко зростає.

Неодноразово висловлювалася думка про те, що із настанням третього тисячоліття лідерство у світі буде оцінюватися не стільки величиною економічного потенціалу, кількістю боєздатних військ чи об'ємом отриманих прибутків країни, скільки її вмінням контролювати інформаційні процеси.

Сучасні досягнення у сфері інформаційних технологій все впевненіше завойовують різні види діяльності суспільства. Останнім часом такий феномен досягнув настільки масштабних розмірів, що життєво-необхідні інтереси держав (особливо у сфері інформаційної безпеки) опинилися під загрозою. Сьогодні під прицілом опинилася перспективна сфера діяльності – професійний спорт. Тому державні системи захисту інформації перебувають у глибокій кризовій ситуації.

Так як проблематика інформаційних війн є надзвичайно широкою, підходи, погляди та різні аспекти надзвичайно активно вивчаються науковцями. На сьогодні представлено багато праць та статей, які присвячені саме специфіці та питанню інформаційних протиборств зокрема. Серед науковців та дослідників, які вивчали цю проблему, а також розглядали її різні аспекти, слід відзначити таких вітчизняних та зарубіжних фахівців як А. Манойло [6], В. Циганов, Г. Почепцов, І. Панарін [7], М. Галамба, М. Лібікі, О. Цвєтков [9], П. Кузнєцов, Р. Шафранський [10], С. Бухарін, С. Расторгуєв [8] та інших. Особливо варто приділити увагу науковим досягненням І. Панаріна, який досліджував інформаційну війну у кількох суміжних аспектах: політика, геополітика та дипломатія [7]. Що ж стосується об'єкту статті, то Інтернет як нове явище в інформаційному суспільстві розглядалося багатьма дослідниками у різноманітних напрямках. Свій внесок у вивчен-

ні глобальної мережі зробили І. Стялова, І. Биков, Л. Іловайська, М. Хейг, які аналізували використання Інтенет-технологій у PR; А. Калмиков, Дж. Гол, Л. Коханова, які розглядали особливості Інтернет у мас-медійному середовищі. Однак П. Ажед, Ф. Бретон, Р. Гордон, Г. Грезійон, К. Керделлан, К. Янг, О. Войскуський у порівнянні з іншими вже конкретніше досліджують Інтернет і розуміють його як чергову інновацію, створену людьми для поліпшення й урізноманітнення життя. Але зараз дуже важко виділити вітчизняних чи зарубіжних дослідників, які б конкретно займалися питанням інформаційних війн та Інтернету. Тому за доцільне вважаю продовжувати дослідження цієї тематики, адже вона є надзвичайно перспективною та актуальною у наш час.

Основним завданням статті є розкриття суті поняття «інформаційна війна» та розгляд його основних складових елементів. Однак в першу чергу потрібно окреслити взаємозв'язок між інформаційним протиборством та Інтернетом, а також дослідити влив нового явища на суспільство.

Інформаційною війною є сукупність методів та способів цілеспрямованого впливу суб'єктів-агресорів в умовах інформаційної відкритості на соціальні відносини (відносини людей між собою, відносини в суспільстві та державі), інформаційні ресурси, інформаційно-аналітичні та інформаційно-технічні системи, системи формування масової свідомості та психіки окремої людини, з використанням усіх властивостей інформації, інформаційних ресурсів та новітніх інформаційно-телекомунікаційних технологій з метою штучного створення факторів гальмування розвитку людини, суспільства та держави, встановлення контролю над інформаційними ресурсами потенційного супротивника задля отримання переваг у пріоритетних сферах суспільного життя [1, с. 6].

Інформаційна війна має два аспекти: технологічний та ідеологічний [8, с. 222-226]. З точки зору першого, мова йде про те, що у визначений час приводяться в дію програмні віруси, логічні бомби, закладені у пам'яті інформаційних комп'ютерних мереж. Вони здатні зруйнувати і знищити програми управління, бази даних, вивести з ладу важливі об'єкти (наприклад, пошкодження роботи з рахунками у зарубіжних банках, заглушення теле– і радіомовлення у певному регіоні, припинення діяльності армійських

пунктів зв'язку і управління). Сьогодні цей аспект використовується дуже часто, адже під час інформаційних війн здійснюються атаки на програмно-технічне забезпечення ворога, тому що це є найбільш ефективним методом «обеззброєння» противника та позбавлення його засобів як нападу, так і захисту.

До ідеологічного аспекту відносять ідеологічну обробку населення, яка призводить до нестабільності політичної ситуації у країні, до дезорієнтації населення і спричинення паніки [8, с. 226-230]. Навіть незначне проникнення інформації з метою забезпечення операції, веде до значних матеріальних наслідків і до забезпечення інтересів більш розвинутої країни. Такий вплив інформації на громадську думку спричиняє спокійне ставлення населення до агресивних кроків і навіть воєнних дій. Неозброєним оком можна побачити, що через засоби масової комунікації при веденні інформаційних операцій та війн впливають на міжрегіональні протиріччя, розпалюють міжетнічну і міжнаціональну ворожнечу, створюють комплекс меншовартості У порівнянні із попереднім аспектом, ідеологічний є набагато серйознішим та небезпечнішим, адже при технологічному завдаються матеріальні та ресурсні збитки, у той час коли ідеологічний здійснює незворотні та шкідливі зміни у психіці, поведінці та цінностях людей, що є незворотнім процесом.

Беручи до уваги попередньовказані факти, слід пам'ятати, що інформаційна війна у порівнянні із звичайною має наступні відмінності:

– Звичайна війна передбачувана і допускає застосування оборонних заходів. У випадку інформаціної війни можливі визначені операції стосовно захисту, «вакцинація» мислення проти введення альтернативної точки зору. У більшості випадків досить тяжко вгадати напрямок та інструментарій можливої атаки. Тобто розрізнити атакувальні чи захисні процеси в інформаційній війні практично неможливо, а інструментарій може варіюватися від кількох до цілого ряду різноманітних типів.

– Під час звичайної війни територія загарблюється повністю; при інформаційній – можливе поетапне захоплення, коли аудиторія завойовується частинами. Можлива окрема робота із лідерами думок, молоддю та іншими впливовими колами суспільства. На

відміну від бомби або іншої небезпечної зброї, яка знищує всіх, інформаційна війна діє вибірково, охвачуючи при цьому різноманітні прошарки населення. Саме через це популярність останньої є надзвичайно високою, так як вона дає можливість без значних зусиль змоделювати конкретний план: обирати та змінювати аудиторію впливу залежно від ситуації.

– При веденні інформаційної війни можливе багаторазове захоплення одних і тих же людей, що виражається в атаці різних тематичних зон свідомості. А отже, це збільшує шанси ефективної маніпуляції над масами. Тому інформаційна війна представляє більшу загрозу у порівнянні із звичайною.

– Людина не в змозі реагувати на невидиму дію (наприклад, радіацію). Більш того, така дія може приймати і доброзичливу форму, на яку біологічно людина ніяк не готова відповідати, навіть агресивно. Тому головна небезпека інформаційної війни – відсутність видимих руйнувань, що характерні для звичайних війн. Суспільство навіть не підозрює, що, воно піддається впливу. Як результат – люди не використовують наявні у їх розпорядженні захисні механізми. Загалом, інформаційна війна виглядає як «мирна», оскільки може вестися на фоні благополуччя та миру [7, с. 93].

– На відміну від війн минулого, простір та відстань не є перешкодою для інформаційних війн, особливо коли їхнім середовищем є Інтернет. Саме він є тим каталізатором, який спрощує та пришвидшує багато процесів, які відбуваються у суспільстві, політиці, економіці та інших сферах життєдіяльності, та дозволяє дистанційно контролювати хід інформаційної війни.

– В інформаціній війні змінюється роль впливу: від суто фізичного (знищення об'єкта, завдання щкоди), до комунікативного. Основним завданням тепер постає зміна комунікативного оточення об'єкта. Війни, що були направлені на завоювання простору, змінилися війнами, які борються за знання. «Інформаційні технології дозволяють забезпечити розширення геополітичних криз, не зробивши жодного пострілу» [6, с. 58-59, 62].

Основними цілями інформаційної війни є бажання контролювати інформаційний простір, при чому захистити власний від негативного впливу ворожих дій (контрінформація); контроль за інформацією для ведення інформаційних атак на ворога;

підвищення ефективності сил спротиву за допомогою всебічного використання основних функцій інформації [3]. В принципі це є загальні та найбільш поширені завдання війни, проте слід пам'ятати, що вони можуть відрізнятися і залежати від певної специфіки тактики чи стратегії протиборства. Наприклад, якщо інформаційна війна ведеться проти конкретної держави, основними цілями буде ініціювання страйків, масових заворушень, інших акцій протесту і непокори; підрив міжнародного авторитету держави, її співпраці з іншими державами; маніпулювання політичною орієнтацією населення для створення політичної напруги та стану, близького до хаосу; зниження рівня інформаційного забезпечення органів влади та управління; введення населення в оману щодо роботи державних органів влади, підрив їх авторитету, дискредитація їх дій, тощо.

За Бережною М. С. поле дії інформаційних воєн є досить широким і охоплює наступні області:

– всесвітня мережа Інтернет;

– системи управління та прийняття рішень (цивільні, військові, соціальні, культурні);

– інфраструктура систем життєзабезпечення держави (системи телекомунікації, енергетики, фінансів, промисловості, транспортні мережі);

– військова інформаційна інфраструктура (системи контролю, управління і зв'язку, розвідка);

– система особистих даних (злам і використання паролів VIP-персон, ідентифікаційних номерів, банківських рахунків, даних конфіденційного плану, виробництво дезінформації);

– система озброєнь і захисту від шпигунства (розкрадання патентованої інформації, спотворення або знищення особливо важливих даних, послуг; збір інформації розвідувального характеру про конкурентів) [2, с. 7-10].

Порівнюючи всі ці області ведення інформаційної війни, найперспективнішим та найактуальнишим сьогодні, звичайно, залишається Інтернет. Адже він володіє низком переваг, якими не можуть похвалитися інші види війн.

Найчастіше інформаційні війни ведуться у політичній, дипломатичній, фінансово-економічній та військовій сферах. Хоча

останнім часом можна стостерігати нову тенденцію – ведення інформаційних атак у сфері професійного спорту. Однак потрібно розрізняти два види таких протиборств: інформаційно-психологічне та інформаційно-технічне. Вони дуже тісно пов'язані із двома аспектами інформаційних війн – ідеологічним та технологічним відповідно. Найважливішими об'єктами впливу і захисту першого є психіка політичної еліти та населення, системи формування масової свідомості та думки, прийняття рішень. Що ж стосується інформаційно-технічного, то це системи передачі даних та системи захисту інформації.

Причин великої популярності інформаційних війн у XXI столітті є безліч, але основними є наступні. Велика різниця у якості та кількості знань представників різних соціальних груп та бажання збагатитися новими цікавими фактами. По-друге, існує непереборне прагнення послабити моральні і матеріальні сили своїх конкурентів з однієї сторони, та посилити власні – з іншої. По-третє, використовуються різні методики впливу (особливо пропагандистські) на свідомість людини. По-четверте, війна є однією з тих важливих складових ідеологічної боротьби, яка завжди є наперед спланованою, узгодженою та цілеспрямованою дією, яка має власну стратегію, цілий набір методів та засобів. Звичайно, її наслідки не обов'язково призводять до кровопролиття, руйнувань або численних жертв. Але така уявна псевдобезпека лише маскує реальні наслідки інформаційної війни, адже вони за своїми масштабами куди серйозніші у порівнянні із звичайними. Як мінімум, це може викликати дискомфорт та стрес, також здійснюється величезний вплив на масову свідомість, руйнується загальна стабільність у багатьох сферах життя. Найгірше, чого варто очікувати, це знищення психології людини, суспільства, нації, різка зміна певних вірувань, узгоджених правил, стереотипів та установок. Тому твердження, що інформаційна війна є спонтанним явищем або результатом випадкових подій, абсолютно помилкове.

Разом із стрімким розвитком новітніх технологій та більшою кількістю таких взаємодій з іншими групами (включаючи внутрішні) або державами, виникають нові та більш ускладнені проблеми, які у подальшому можуть призвести до інформаційної війни. Тому можна вважати, що висока довіра людства до новинок у сфері сучасних технологій є однією з властивих слабких місць. І ця вразливість буде зростати по мірі збільшення кількості мереж або об'єму транзакцій.

Більшість науковців та дослідників дають доволі подібні визначення поняттю «Інтернет», як глобальна комп'ютерна система:

– логічно взаємопов'язана середовищем глобальних унікальних адрес (кожен комп'ютер, підключений до мережі, має свою унікальну адресу);

– здатна підтримувати комунікації, здійснювати обмін інформацією;

– забезпечує роботу високорівневих сервісів/служб (чати, відео конференції, електронна пошта та ін.) [5, с. 54-62].

У наш час Інтернет вважається більше, ніж просто всесвітня мережа. Перш за все, це зручний та швидкий засіб комунікації з користувачем, по-друге, це глобальне джерело інформаційних ресурсів, по-третє, це світова мережа багатьох зв'язків, яка об'єднує мільйони користувачів комп'ютерів великої кількості країн у єдине ціле.

Беззаперечними перевагами у звичайному використанні Інтернету є висока швидкість передачі та отримання інформації, відносна дешевизна, необмеженість аудиторії, анонімність, масивний об'єм даних та багато інших. Однак під час ведення інформаційної війни існують інші, не менш важливі переваги глобальної мережі:

Прихованість джерела впливу. Завдяки цій перевазі кожен анонімний проксі-сервер може безперешкодно атакувати ресурси в Інтернеті, так як такі акти агресії надзвичайно важко відрізнити від дій звичайних комп'ютерних хуліганів. Підготувати та провести такий кібернапад може досить широке коло осіб – від військових і розвідувальних структур іноземних держав, до партизанських формувань, злочинців, промислових конкурентів і хакерів.

Оперативність. Завантаження і регулярне оновлення даних на блогах, веб-сторінках, форумах, різного роду інтернет-виданнях та новинних порталах, у порівнянні із звичайними споживачами, дає можливість користувачам отримувати інформацію у режимі

реального часу. Крім того, сама підготовка та оформлення матеріалу в електронному вигляді займає небагато часу, що значно збільшує ефективність і швидкість ведення інформаційної війни.

Економічність. Для звичайної інформаційної атаки достатньо залучити як мінімум підготовленого користувача персонального комп'ютера (що підключений до телефонної лінії) або ж невелику кількість персоналу та матеріальних засобів для вирішення поставлених завдань. У порівнянні із звичайною війною, застосування комп'ютерних технологій дає значно більший ефект та істотно менші витрати.

Дистанційний характер впливу на комп'ютерні системи у різних регіонах світу. Прикладом такої переваги може бути атака комп'ютерної системи одного з каліфорнійських операторів, яка здійснювалася навесні 2001 року на території однієї з провінцій Китаю через американські веб-сервери, що розташовані в трьох містах США. Цей кібер-напад виявили лише через 17 днів.

Масштабність можливих наслідків. Окрім впливу на формування громадської думки, деструктивної дії на позиції офіційних осіб, які приймають найважливіші рішення, використання Інтернету може призвести до порушення балансу функціонування деяких елементів або тривалого виведення з ладу життєво необхідних об'єктів і систем в окремих районах, країнах або регіонах.

Комплексність інформації та її сприйняття. На веб-сайтах можна розміщувати як текстову, так і графічну інформацію, а її обсяг може у сотні разів перевищувати об'єм будь-якого друкованого видання, радіо- або телепередачі. Використання сучасних мультимедійних технологій дозволяє одночасно здійснювати вплив на декілька органів чуття, що має додатковий емоційний вплив.

Доступність інформації. За словами Хамадуна Туре, генерального секретаря Міжнародного союзу електрозв'язку (спеціалізована установа ООН), загальна кількість користувачів Інтернет на початку 2011 року сягнула двох мільярдів. У лічені секунди будь-хто безперешкодно отримує доступ до інформації, яка належить різним країнам, нехтуючи при цьому прикордонними, цензурними та інші бар'єрами [4].

Можливість дезінформувати здійснюється шляхом розсилання електронних листів, розміщення постів на форумах, блогах, організації новинних груп, створення соціальних мереж для обміну думками, розміщення інформації на офіційних веб-сторінках певних організацій [5, с. 60-78].

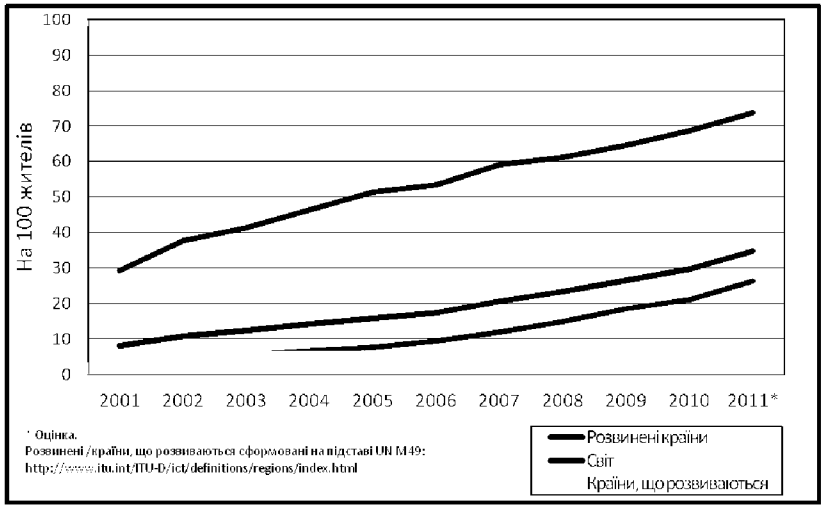

Рис. 1. Кількість Інтернет користувачів на 100 жителів, 2001-2011*

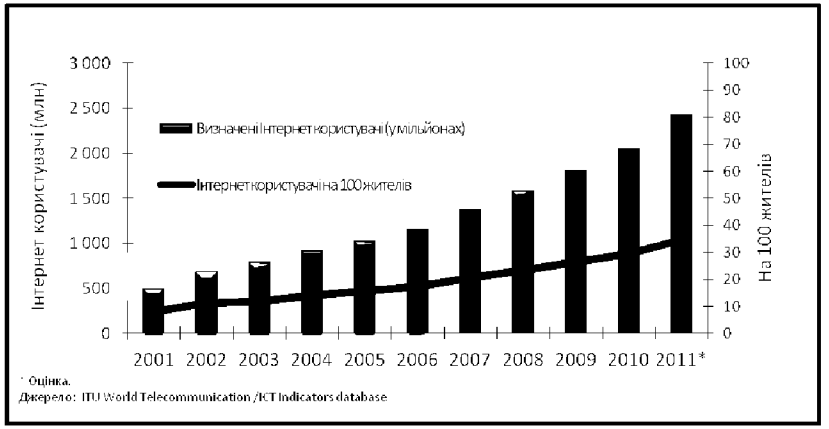

Рис. 2. Кількість Інтернет користувачів у світі, загальна та на 100 жителів, 2001-2011*

За період 2000-2011 число користувачів Всесвітньої мережі зросло майже у три з половиною рази, тобто на червень 2011 року їх кількість становила 353.1% від кількості 2000 року (рис. 1, 2). Найбільш потужними країнами-користувачами Інтернет є Німеччина, Росія, Велика Британія, Туреччина. Україна посідає 9 місце у списку (більше 15 млн. юзерів) [11]. А це означає, що із збільшенням кількості користувачів Інтернет виникає серйозна проблема контролю відкритих даних, а також зростає загроза переростання звичайних конфліктів у жорстку інформаційну війну.

Отже, під інформаційною війною потрібно розуміти різносторонню і цілісну стратегію, яка спричинена підвищеною значущістю і цінністю інформації у сфері політики, економіки, оборони та безпеки держави. Дуже часто у ході такої боротьби використовуються переваги технологічних вдосконалень і досягнень сьогодення, зокрема Інтернет. Основною зброєю такої боротьби вважаються повідомлення ЗМІ та нетрадиційних джерел інформації, що використовуються для широкомасштабного, цілеспрямованого, швидкого та таємного впливу на цивільні, військові, економічні та державні загалом інформаційні системи противника). Найновішою формою війни сьогодення вважається інформаційна війна, об'єкт якої базується на можливості підкорення волі людини, управління знаннями та маніпулювання суспільною свідомістю. Основна небезпека такого протиборства полягає у різкому збільшенні масштабу бойових дій за рахунок глобальної мережі Інтернет, а також у тому, що такий вплив здійснюється ірраціонально та приховано, тому виявити інформаційно-психологічну дію вдається не одразу і не завжди.

Літреатура:

1. Абакумов, В. М. Суб'єкти інформаційних війн : поняття та види / В. М. Абакумов // Форум права. – 2009. – № 2. – С. 6-12. – [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2009-2/09avmptv.pdf. – Назва з екрана.

2. Бережна, М. С. Теоретичні концепції інформаційних війн США кінця XX – початку XXI ст. / М. С. Бережна // Гілея : наук. вісн. – 2010. – №34. – С. 220-229. – [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Gileya/2010_34/Gileya34/I22_doc.pdf. – Назва з екрану.

3. Информационные войны. Введение [Электронный ресурс]. – Режим доступа : URL. http://vladimir.socio.msu.ru/1_KM/theme_13.htm#top. – Название с экрана.

4. Кількість користувачів Інтернетом уже перевищила 2 млрд [Електронний ресурс] / Є. Борисов. – Режим доступу : URL. http://www.newsmarket.com.ua/2011/01/kilkist-koristuvachiv-internetom-uzhe-perevishhila-2-mlrd/. – Назва з екрану.

5. Кубко, В.П. Документна лінгвістика. Конспект лекцій для студентів спеціальності 7.020105 – документознавство та інформаційна діяльність денної та заочної форм навчання [Текст] / В. П. Кубко. – Одеса : Наука і Техніка, 2007. – 92 с.

6. Манойло, А. В Государственная информационная политика в условиях информационно-психологической войны [Текст] / А. В. Манойло, А. И. Петренко, Д. П. Фролов. – 2-е изд., стереотип. – М. : Горячая линия-Телеком, 2007. – 541 с.

7. Панарин, И. Н. Технология информационной войны [Текст] / И. Н. Панарин. – М. : «КСП+», 2003. – 320 с.

8. Расторгуев, С. П. Информационная война. Проблемы и модели [Текст] / С. П. Расторгуев. – М : Радио и связь, 1999. – 416 с.

9. Цвєтков, О. Інформаційна війна в Інтернеті / О. Цвєтков // Перехід IV. – 1999. – №2. – С. 57-62. – [Електронний ресурс]. – Режим доступу : http://www.perehid.org.ua/16.html. – Назва з екрану.

10. Szafranski, R. A Theory of Information Warfare. Preparing For 2020 [Text] / R. Szafranski // Airpower Journal. – 1995, Spring. – №9. – P. 58-59, 62.

11. World Telecommunication / ICT Indicators Database. Internet users. [Electronic resource]. – Mode of access to URL: http://www.itu.int/ITU-D/ict/statistics/. – A title from screen.