UDC 325.744

Volodymyr Grubov

Doctor of Political Sciences, Professor, Research Center for Humanitarian Problems of the Armed Forces of Ukraine, street of Narodnogo Opolchennya 5a, Leading Researcher,

e-mail: GrubovVM@gmail. com

CONTROLNET: THE AMOUNT OF TECHNOLOGIES IN THE SERVICE OF LARGE POLICY

Abstract

Today the sumof technologies embodies the universal principle, which destroys the world of traditional representation sofhuman consciousness about the bound ariesof the necessary and possible assymbolic linesof division between good and evil, security and threat, anonymity and publicity.

The relevance of the subject determines logosphere technologization of growing human existence that produces the negation of things existing and new information capabilities makes most people very vulnerable and dependent on them. Especially it is realized when technologies are resource policies and government to achieve common interests and the common good.

The article is an attempt to analyze the key problems of latent practices of leading countries — the US, Russia and China's control over «information man» life within national jurisdiction information space through information technology.

It emphasizes that with increasing information leading power in world politics security becomes subject of plane rotations both in open and closed day agenda. It is a national information space monitoring and control screening function of the state to neutralize the negative factors of the internal opposition and the pressure of circumstances, which dictates a new global information reality. The main trend that reality consists of challenges and threats related to the use of information resources, which classified information and psychological operations, information aggression, cyber terrorism and cybercrime.

It attempts to look at information technology and thinking that they formed as a tool which «transforms man into the system functions», cog of information society and the all-powerful state machine. Developing the idea of human space automation, the system gradually developed a habit of living «seamlessly», «comfortable» and «separately». However, entering into every house as «good» human rationality, technology has become a hostile force that has to control everything and everyone. Man is helpless, and his life is completely transparent.

Separately it analyzes control policy of information space and Internet space of USA, Russia and China, which is within national strategies for information security. It underlines the common features and distinguishes features of this policy which are dictated by the level of the national sector of the information economy and the level of implementation of security projects of national and global level.

Asitisconcluded in the condition sofin creasing the risks and challenges of the informationen vironmentandinorderto preservesocio-political stability of society, state sthatactas historically veri fiedguardians of social peace will seekto use information technologiesas a latent toolkit for monitoring private life of citizens. As a resource of information security policy, this toolkit all owstotrack negative social trends and respondin a timely way to the irmani festations from the point of view of national interests. First of all, it concerns the risks of making decisionsre latedto terrorist and extremist threats that have become a dangero usside of the life of a modern person.

Keywords: information space, information security, information technologies, cyberspace, national interests.

УДК 325.744

Грубов Володимир Михайлович

Доктор політичних наук, професор Науково-дослідний центр гуманітарних проблем Збройних Сил України, вул. Народного Ополчення 5а, провідний науковий співробітник,
e-mail: GrubovVM@gmail. com

CONTROLNET: СУМА ТЕХНОЛОГІЙ НА СЛУЖБІ ВЕЛИКОЇ ПОЛІТИКИ

Резюме

Завдяки комп'ютерним технологіям людина стає одночасно і вільною, і вразливою, успішною і слабкою. Особливо це стає помітним, коли в ці процеси втручається стороння сила, яка використовуючи їх можливості створює знайому ситуацію «панoптикуму», коли приватне життя людини набуває майже абсолютної прозорості. Цією силою виступає держава.

Метою і завданнями дослідження є спроба прояснення латентних практик провідних країн світу — США, РФ і Китаю щодо контролю за життям «інформаційної людини» в межах як національного, так і міжнародного інформаційного простору.

Встановлено, що в політиці контролю національного сегменту кіберпростору, яку проводять уряди США, Росії і Китаю існують як загальні, так і особливі риси, які, перш за все, відповідають національним стратегіям безпеки. На відміну від РФ і Китаю, які інформаційні технології переважно розглядають як чинник забезпечення безпеки і оборони, в США це питання ставиться значно ширше — інформаційні технології повинні забезпечити світове лідерство США в усіх сферах життя. Проте, пріоритет віддано безпеці економічній і, відповідно, збереженню і захисту таємниць економічного характеру. Загальним є те, що в політиці забезпечення безпеки країни відштовхуються від нових світових реалій, які формують нові виклики і тенденції, ступеня довіри у міжнародному політичному просторі і стану двосторонніх відносин. У переліку нових викликів відкритий інформаційний простір де спілкуються вільні особистості стає неабияким фактором поля невідомих ризиків, які ці країни прагнуть локалізувати і взяти під національний контроль. На практиці це означає «слухати всіх і всюди». Головною проблемою в трикутнику США — РФ — Китай залишається питання інформаційної безпеки на рівні міждержавних відносин, яку сторони розглядають як суму певних правил гри.

У якості висновку зазначається, що як ресурс політики інформаційної безпеки держави інформаційні технології стають основою латентного інструментарію контролю за процесами в суспільстві, що дозволяє відслідковувати суспільні тенденції негативного характеру і реагувати на них з позицій національних інтересів.

Наведений аналіз дозволяє нам акцентувати увагу на питанні співвідношення особистісного і загального (суспільного), де Інтернет свобода особистості і можливості комп'ютерних технологій як нових складових екзистенційного підгрунття безпеки потребують більш глибокого осмислення людською особистістю канонів відносин у такій чутливій системі як «Я і МИ», що відповідає природі самозбереження зрілого розуму.

Ключові слова: інформаційний простір, інформаційна безпека, інформаційні технології, кіберпростір, національні інтереси.

1. Вступ

Переконливим фактом нашого сьогодення є те, що на наших очах відбувається інформаційна реконструкція канонів багатьох соціальних і гуманітарних наук, завдяки якій вони перестають сприйматися як вічні і безперечні здобутки людської раціональності, головним завданням, якої завжди було орієнтація суспільної свідомості на збереження цілісності і органічності буття людини. Наслідки втрати єдності чуттєвого і раціонального, відлік феномену якої розпочав «чистий розум» І. Канта, у наші дні матеріалізувався в «духовній регресії» [1, с. 98] і «відхиленій раціональності», де закарбована в інтерес Аристотелівська логіка «техне» породжує людину нескінченного «інформаційного потягу». Для такої людини цікавим є не стільки само знання як продукт чистого розуму, скільки логіка його отримання через наявний технологічний інструментарій. Звідси, постулати попереднього знання, сьогодні виглядають не як логічні результати раціональності попередніх поколінь, а як певні парадокси. Таку картину ми спостерігаємо коли, наприклад, чуємо твердження, що кордони геополітики охопили кіберпростір; що промислова фірма є успішною, якщо вона є «швидкою», а її продукт «легким»; що трансгранична соціалізація (дистанційне навчання, робота, розваги) робить зв'язок з «землею» надто примарним і нестійким, що будь-яка талановита людина може стати «сам-собі» фірмою не покидаючи простір власної квартири тощо. Причиною таких трансформацій є зростаюча технологізація логосфери буття людини, яка продукує різнорівневість категоріального становлення знання. Internet можливості й інформаційні технології стали своєрідним запереченням наявного порядку речей як в сфері наукового знання, так і в сфері соціальних відносин, де прагнення держави «всі успіхи розсудку» [2, с. 230] поставити на служіння державній машині, заходить у пряме протиріччя з природними правами самої людини і правилами міждержавних відносин. Картину нової реальності дозволяє осягнути слоган «сума технологій», який вперше запропонував в однойменний праці С. Лем [3]. З ним він пов’язав всі перспективи, успіхи і виклики людській цивілізації. Сьогодні сума технологій уособлює універсальний принцип, завдяки якому руйнується світ традиційних уявлень людської свідомості про кордони необхідного і можливого як символічних ліній поділу між добром і злом, безпекою і загрозою. Розширивши реальність і деанонімізував інформаційний простір буття людини, технології зробили його відкритим і прозорим, а саму людину надто вразливою. В інформаційних технологіях відхилена раціональність повстає загрозливою субстанційною реальністю, у викликах якої людина губиться та втрачає свою самість і відчуття безпеки. Адже в інформаційній реальності вона одночасно і господар, і об’єкт щоденного контролю.

Аналіз останніх джерел та публікацій показує, що незважаючи на достатньо широке коло досліджень проблем інформаційної безпеки особистості, загальний дискурс цих робіт присвячений переважно конституційно-правовим аспектам діяльності органів державної влади і виконанню ними взятих на себе міжнародних зобов’язань. Цим питанням присвячені праці Кузьменко А., Кулагіна К., Судакова О., Манойло А., Петренко А., Фролова Д., Ліпкана В., Максіменко Ю., Желіховського Л., Марущака А., Евтихевича Н., Олійника О, Сосніна О, Шиманського Л., Дзьобаня О., Штанько В., Тіхонова Л., Дубова Д., Ожевана М., Садовнічого В., Лазарева І., Бейліна М., Чернова А., Гуза А., Пилипчука В. та ін. Проте проблема інструментального (технологічного) втручання держави в інформаційний простір особистості і слідкування за допомогою інформаційних технологій за її власним життям висвітлена ще недостатньо.

2. Методи дослідження

Метою і *завданням* статті є спроба розкрити латентні практики провідних країн світу — США, РФ і Китаю щодо контролю за життям «інформаційної людини» в межах як національного, так і міжнародного інформаційного простору на основі аналізу нормативно-правових актів цих країн і застосовуємих ними інформаційних технологій. Для досягнення мети були використані такі ***методи***: діалектичний, системний, аксіологічний, компаративний.

3. Результати

Найбільш дискурсивними питаннями сьогодення у функціонуванні національного і міжнародного інформаційного простору є інформаційна безпека держави, інформаційна безпека особистості, кібербезпека і зміцнення міжнародної довіри і безпеки при використанні інформаційно-комунікативних технологій (ІКТ). Артикульовані в інформаційний простір положення не викликають особливих питань до тих пір, поки вони не стикаються з його розумінням або як «ресурсу», або як «поля» [4]. Більш глибока за змістом проблематика стає очевидною, коли питання інформаційної політики починають реалізовуватися у національних практиках, які як правило, оперують категоріями «протистояння», «боротьби» і «захисту інтересів». Зміна модальностей призводить до акцентуалізації в політико-інформаційному дискурсі тем попередження крадіжок і захисту інформації; забезпечення цілісності і функціональності інформаційної інфраструктури; захисту баз даних; нейтралізації інформації деструктивного характеру; моніторингу національного інформаційного простору та його правового захисту. Така реакція є свідченням, що з зростанням інформаційної потуги лідерів світової політики, безпекова тематика набуватиме обертів у площині як відкритої, так і у площині закритої повістки дня. Йдеться про моніторинг національного інформаційного простору і контрольно-скринінгову функцію держави з метою нейтралізації негативних чинників внутрішнього розвитку і протистояння тиску обставинам, які диктує нова глобальна інформаційна реальність. За визнанням експертної спільноти її головну тенденцію складають виклики і загрози пов'язані з використанням інформаційного ресурсу, до якого віднесено інформаційно-психологічні операції, інформаційна агресія, кібертероризм і кіберзлочинність [5, с. 236–237].

В першу чергу вони пов'язані з інформаційним суперництвом і складностями врегулювання інформаційних відносин як на міждержавному, так і на державному рівні, якій формують різноманітні суб'єкти інформаційних відносин. Зрозуміло, що у міжнародному інформаційному просторі головними з них є інформаційні транснаціональні корпорації, наприклад, як Microsoft, Google, Yahoo, Facebook, Youtube, Apple тощо, які за підтримки держави переслідують не тільки комерційні, але й далекоглядні цілі «великої політики» самої держави. Такий симбіоз інтересів побудований на основі технологічного домінування і «функціонального мислення» відхиленної раціональності як звички діяти саме так і саме у такому ключі. Ця звичка виступає у якості перевіренної лінії поведінки цієї раціональності як феноменології технологічних проривів від минулого до майбутнього, що здійснили провідні країни західної спільноти в епоху постіндустріалізму. «У функціональному мисленні присутня сила, яка сприяє просуванню і розповсюдженню автоматизму…За ним стоїть агресивна хватка, безжалісність яку мало хто усвідомлює повною мірою. Це один з самих холодних винаходів раціонального розуму, який керує технічним прогресом» [6, с. 133]. Така думка Ф. Юнгера спонукає нас подивитися на інформаційні технології і спосіб мислення, які вони сформували як на інструмент, який «перетворює людину в систему функцій», «вінтик» інформаційного соціуму і всевладної державної машини. Отехнізовуючи людський простір, ця система поступово виробила звичку жити

«безпроблемно», «зручно», «комфортно» і «відокремленно». Однак, увійшовши в кожен дім блага людської раціональності перетворилася у ворожу силу, яка стала контролювати все і всіх. У якості футурологічного проекту цей феномен у вигляді «великого брата» переконливо описаний у Дж. Оруела у його відомій праці «1984». Сьогодні прикмети цієї реальності дещо розширилися. Важелі телевизора доповнили смартфон й Internet, а сучасна інформаційно-правова практика ці тенденції лише підтверджує. «Закрита повістка дня», де діяльність держави залишається поза увагою громадянського суспільства вже давно стала нормою життя інформаційних спільнот і прикладом такої реальності є політика інформаційної безпеки США, Російської Федерації (РФ) і Китаю.

У колі сучасних світових лідерів США є першою країною в політиці безпекотворення якої, інформаційна сфера була визнана критичною. Прийнятий у 1906 році закон «Про захист інформації», який упорядкував, перш за все, питання поводження з інформацією комерційно-виробничого характеру, в подальшому визначив коло питань більш державницького значення. Йдеться про Закон «Про національну безпеку» від 1947 року, завдяки якому було здійснене правове периформатування всього інформаційного законодавства. Внаслідок цього, починаючі з 1974 року, США отримали чітку правову систему, де діють понад 500 базових федеральних законодавчих актів, які спрямовані на захист державної таємниці і впорядкування діяльності різноманітних резидентів щодо захисту інформації конфидиційного і комерційного характеру.

Проте, дійсний характер закону «Про національну безпеку» США визначили не стільки відкриті салогани і модальності, якими він оперував, скільки та особлива функція, яка була покладена на органи державної влади і підпорядковані їм структури, які відповідатимуть за захисту інформації. Контроль і стеження за фізичними і юридичними особами, чия діяльність могла спричинити небезпеку національним інтересам США стали основою документу і визначили його зміст. У коло таких осіб підпадали як іноземці, так і громадяни США, причому географія стеження за цими особами (включно й іноземців) стала носити екстериторіальний характер. У подальшому принцип екстериторіальності США розповсюдили на весь світ, що означало що будь-хто може підпасти під норми законодавства США з відповідними наслідками.

Постановка питання у такій площині стала свідченням того, що інформаційна безпека США набула екстериторіального характеру і стала розглядається як глобальна проблема, якій Америка повинна протистояти. З моменту прийняття закону «Про національну безпеку» інструментом вирішення цієї проблеми стала система глобального стеження «Ешелон» (1947), головним завданням якої стало збір інформації політичного, воєнного і економічного характеру. З часом в коло цих завдань були включені питання стеження за фізичними і юридичними особами, чия діяльність теж підпадала у розряд «небезпечних».

Проект «Ешелон» мав декілька етапів розширення кола його учасників. Перший етап охопив англомовний світ — це США, Великобританію, Канаду, Австралію і Нову Зеландію. На другому етапі до нього приєдналися Німеччина, Данія і Туреччина (уряди цих країн надали свої території для встановлення на них наземних станцій перехоплення і стеження). На третьому етапі членами проекту стали Італія, Японія, Швейцарія та ще низка країн Північної Африки і Близького Сходу, які теж надали свої території для розміщення наземних і космічних станцій перехоплення інформації [7, с. 68–70].

З розвитком космонавтики проект отримав нове життя. Національне космічне Агентство США NASA і Європейській проект «Інтелсат» дозволяє США контролювати глобальний ринок зв'язку і накопичувати інформацію, яка уявляє інтерес для уряду

США. На сьогодні «Ешелон» дозволяє перехоплювати майже 99% всієї інформації, яка розповсюджується по різноманітним каналам комунікації, причому до 70% всієї інформації носить воєнний і економічний характер [7, с. 70–71].

Загальне керівництво проектом очолює Агентство Національної безпеки (АНБ) США. Незважаючи на те, що проект носить коаліційних характер, тобто є закритою формою співпраці, доступ до всієї інформації у повному обсягу мають лише дві країни — це США і Великобританія. Це пояснюється особливими відносинами між двома країнами, які склалися після Другої світової війни і зацікавленністю Великобританії використовувати ресурси проекту для збереження своєї колоніальної імперії під назвою «Британська Співдружність». Завдяки «Ешелону» США і Великобританія стежать за всіма своїми союзниками і партнерами як потенційними контр гравцями на світовій арені. Наприклад, протягом останніх 7 років під стеження попали глави держав Німеччини, Італії, Франції, Греції та інших країн. Цю інформацію неодноразово оприлюднював Е. Сноуден, колишній співробітник АНБ США і Дж. Ассандж — один з організаторів проекту «WikiLeaks» [8, с. 16–17].

Проект «Ешелон» доповнює комплекс довгострокових заходів контррозвідувального характеру. Вони здійснюються в межах програм «Контррозвідувальна програма США», «Національна стратегічна програма безпеки» та проекту OPSEC («Operation Security»), який націлений на збереження державної і комерційної таємниці та збереження конкурентоспроможності американських компаній. Американська програма забезпечення безпеки виходить із твердження: «Що добре для «Дженерал моторс», те добре і для США». Тому практичні кроки контррозвідки полягають у наданні допомоги американським компаніям у захисті секретів як від ворогів, так і від друзів. З цією метою до складу керівництва великих американських компаній входять колишні співробітники ЦРУ і ФБР, які продовжують підтримувати зв'язки зі своїми спецслужбами. Це сприяє поліпшенню контррозвідувального режиму і прозорості діяльності компаній у сфері захисту інформації. Проте, незважаючи на такі заходи, остаточно вирішити цю проблему не вдається. Її гостроту визначають декілька мільярдів доларів, які щорічно витрачають американські компанії через «діяльність» іноземних конкурентів і розвідслужб. У багатьох випадках економічну і технологічну інформацію вони «знімають» з комп'ютерів і систем зв'язку, якими користуються суб'єкти економічної діяльності.

Гуманітарний аспект інформаційної безпеки в США теж має багато темних сторін, які в експертній спільноті викликають масу зауважень. Повідомлення ЗМІ про існування низки національних і міжнародних проектів, в межах яких вже тривалий час відбувається збір інформації про фізичних і юридичних осіб звернули увагу суспільства на зростаючу проблематику в інформаційних відносинах між державою і громадянином. Як констатує М. Бейлін «аналіз нормативно-правової бази забезпечення інформаційної безпеки і фактичне співставлення її з фактичним положенням справ дозволяє констатувати, що в тріаді «держава-суспільство-людина» в найбільш уразливому стані опиняються фізичні особи» [7, с. 68].

На підставі закону «Про національну безпеку» від 1947 року і за допомогою системи стеження «Ешелон» (1947), про що йшлося вище, США перетворилися на глобального кіберполіцейського, головним завданням якого стало збір інформації про фізичних і юридичних осіб, чия діяльність може спричинити небезпеку або загрозу національним інтересам США. Причому національні інтереси тлумачаться надто широко: від ризиків втратити вигідний контракт (лобіювання інтересів національних корпорацій, які зв'язані з урядом), до контролю за постачанням зброї країнами-конкурентами у будь-який регіон світу, де присутні інтереси США. Відповідно до проголошених норм права у коло таких осіб підпадають як іноземці, так і громадяни США. Причому, геогра-

фія стеження за такими особами стала глобальною, а зміст інформації, яка збирається в автоматичному режимі, у багатьох випадках, визначається як за ключовими словами й їхньою інтерпретацією (тероризм, зброя, війна, акція тощо), номерами телефонів, факсів, так і за тембром голосу і картинками з гаджетів осіб, за якими відбувається стеження [9]. Інформаційні технології, які використовуються «Ешелоном» дозволяють за біометричними даними і «голосовим портретом» відстежувати будь-яку людину у будь якому куточку планети.

У систему «Ешелон» закладені технології, за допомогою яких можна здійснювати взлом повідомлень, які мають високий ступень захисту. Завдяки таким можливостям практично всі електроні пристрої, які побудовані на проходженні електричного сигналу починаючи з електронної пошти, телефону, телексу і закінчуючи Internet перетворюються на «інформаційний простір», який зондується «Ешелоном» у реальному часі. Це надало можливість вже сьогодні на кожного громадянина США і Європи у базах «Ешелону» відкрити індивідуальне електронне досьє, куди заноситься вся інформація, яка знаходиться в державних або приватних базах даних з обмеженим доступом: від медичних закладів, страхових компаній і банків до сайтів, на які періодично «заходить» Internet користувачі. Система побудована так, що за командою оператора вся ця інформація може бути надана у будь-який момент, а сама вона має «вічний» термін зберігання [7, с. 71].

В особливо небезпечному стані знаходяться люди, які всі «таємниці» свого особистого життя довіряють Internet. Демократичність і відкритість цього всесвітнього проекту губиться у специфіці його функціонування і можливості тотального контролю з боку урядових структур і спецслужб США. Як країні-засновнику цього світового проекту США практично належать всі права щодо його регулювання. Реальний контроль за технічною частиною функціонування мережі здійснюється корпорацією ICANN та організацією IANA (Internet Assigned Numbers Authority), які тісно пов'язані з державними структурами США. Принциповим моментом цього питання є те, що ICANN зберігає контроль над кореневими серверами DNS (Domain Name System), через які переважно здійснюється маршрутизація Internet. Технічні стандарти роботи Internet теж встановлюються двома іншими фірмами, розташованими у США IETF (Internet Engineering Task Forse) та IAB (Internet Architecture Board) [10, с. 168]. Така організація і технічна специфіка фукнціонквання Internet робить його важливим ресурсом у контрольно-скринінговій діяльності спецслужб США за всіма його резидентами, де б вони не знаходилися.

У межах Агентства національної безпеки (АНБ) США вже тривалий час працює проект PRISM, за допомогою якого спецслужби відстежують всіх користувачів Internet і характер інформації, якою вони користуються. Система PRISM збирає інформацію з серверів Microsoft, Google, Yahoo, Facebook, Youtube, Skype, AOL, Apple і сервісу обміну текстовими повідомленнями Paltalk. Використовуючи отримані повідомлення можна сформувати досить достатньо повну картину діяльності активного Internet користувача: де він перебуває, з ким він спілкується, які його схильності, характер інформації, якою він користується тощо [11]. Така політика тотального контролю можлива лише за двох умов: якщо вона погоджена з всіма гілками влади США і якщо до цієї діяльності залучені провідні Internet корпорації США. Те, що це відбувається саме у такому ключі свідчать матеріали, які періодично з'являються у ЗМІ і документальні підтвердження Е. Сноудена. Microsoft, Google, Yahoo, Facebook, Youtube, AOL, Apple були залучені до співпраці з АНБ, ФБР і ЦРУ у різні періоди починаючи з 2007 року. Наприклад, у 2011 році компанія Microsoft надала у розпорядження спецслужб свій сервіс Skype, завдяки чому спецслужби (і не тільки США) можуть прослуховувати розмови, читати переписку і визначати місцеположення абонентів ресурсу [12].

На відмінну від США у контрольно-скринінговій діяльності в інформаційній сфері безпеки Російська Федерація (РФ) володіє більш меншими можливостями. Проте, в останні 10 років в цій сфері вона зробила досить багато, чим викликала занепокоєння у спецслужб США. У новітній історії РФ основу цієї діяльності сформували два важливих закони — Закон РФ «Про інформацію, інформатизацію та захист інформації» (1995) і Закон РФ «Про державну таємницю» (1993 р., зі змінами від 06.10.1997 р.). На основі цих законів була створена Міжвідомча комісія із захисту державної таємниці, на яку було покладено завдання координації діяльності органів державної влади із захисту державної таємниці та визначені відповідні функції. Серед органів федеральної виконавчої влади провідну роль в цій справі було покладено на Федеральну службу безпеки Російської Федерації. У ФСБ безпосередньо для виконання покладених завдань було створено підрозділи економічної контррозвідки і контр-розвідувального забезпечення стратегічних об'єктів. Певне відношення до цієї роботи мають підрозділи контр-розвідувальних операцій і деякі підрозділи забезпечення. Починаючи 2017 року до цієї роботи були залучені Війська інформаційних операцій. Про їх створення у лютому місяці офіційно заявив міністр оборони РФ С. Шойгу.

В Російській Федерації національні особливості політики забезпечення інформаційної безпеки базуються на декількох важливих документах — це Стратегії національної безпеки РФ до 2020 року і Доктрині інформаційної безпеки РФ. З точки зору заявленної теми в цих документах проглядаються два чітко сформованих напрямки діяльності держави — це використання технологій, якими вже оперує міжнародна практика і сприяння розвитку власної інформаційно-технологічної бази. Характерним прикладом реалізації першого напрямку може слугувати російська космічна система «Глонас» і супутникова система зв'язку на базі апаратів «Гонець» і «Космос 2416», які дозволяють РФ контролювати міжнародний простір зв'язку і позиціонування «потрібних» об'єктів на рівні з такими системами як «Ешелон» і «GPS», які створено у США. Щодо другого напрямку, то тут вирішальний крок Росія зробила у 2010–2015 роки. Справа у тому, що на початку 90-х років компанію Microsoft як провідного виробника операційних систем, запідозрили у «закладках», які вона свідомо робила у «программному» продукті з метою подальшого зняття інформації з комп'ютерів і використання її у власних цілях. Загроза несанкційного доступу до інформації підштовхнула уряд РФ до прийняття рішення про налагодження власного виробництва операційних систем і переходу на ці системи всіх державних органів влади і секторів економіки, які з точки зору національної безпеки є критичними. З метою прискорення цієї роботи з 2014 року в державних органах влади Росії заборонено будь-які сервіси Google, планшети iPad і закупівля програмних продуктів закордонного виробництва [11;12;13]. На додаток на інформаційному ринку Росії з'явилася досить успішна компанія «Лабораторія Касперського», яка виробляє конкурентний продукт щодо захисту інформації й інформаційних систем. Нададаток, як свідчать аналітики, на фоні такої специфіки, лабораторія стала офіційним інструментом влади у контролі за резидентами національного інформаційного простору, де вона органічно доповнює вже існуючи державні проекти.

Найвідомішим з них є СОРМ («Система технічних засобів для забезпечення функцій оперативно-розшукових заходів»), який запущено з середини 90-х років минулого століття. На його базі створено СОРМ–1 (1996), який забезпечує прослуховування всіх розмов по телефону і СОРМ–2 (2000), який забезпечує контроль за діяльністю Internet мережі [7, с. 70–71]. Відповідно чинному законодавству РФ оператори сотового зв'язку повинні зберігати інформацію про паспортні дані абонента; з'єднання, трафік і номера абонентів; факти Internet сесій. Законодавчо перелік цих вимог коригується в залежності від оперативних потреб. Наприклад, з'явилася норма, яка

вимагає зберігати інформацію про Internet трафік протягом трьох років. Як свідчать експерти в РФ практично вже створено систему централізованого збору і збереження персональної інформації, яка зберігає інформацію з різноманітних джерел про всіх громадян країни.

У здійснені концепції «контрольованого суб'єкту» в межах інформаційної безпеки держави і людини, Китай займає особливе місце. Увагу до цього питання з боку влади Китаю можна пояснити двома факторами. Перший фактор пов'язаний з кількісними величинами — це кількість користувачів Internet в країні. За офіційними даними влади у 2013 році вона склала 538 млн. людей, що майже дорівнює сумі всіх користувачів Internet, які зареєстровані в ЄС і США (ЄС — 368 млн., США — 245 млн.). Якщо взяти до уваги динаміку зростання китайського сегменту Internet, то у ближчі 10–15 років ця цифра перевищить 700 млн. людей. Другий фактор пов'язаний з цивілізаційним протистоянням Сходу і Заходу, ядром якого є сфера чуттєво-духовного світу людини. Для влади Китаю боротьба за контроль над комунікативним інструментарієм й інформаційними простором є головною проблемою у збережені цінностей китайської культури у цивілізаційному протистоянні з Заходом. У контексті цієї проблеми у січні 2013 року в «Женьмінь Жібао» — центральному органі ЦК КПК була надрукована стаття Ван Ївея присвячена протистоянню ціннісних моделей розвитку сучасної світової цивілізації. Автор доводить думку, що «людство потребує глобалізації іншого порядку, глобалізації системи цінностей, яка в межах всього світу поважатиме і виражатиме багатомаїття та багатство різних цивілізацій» [14].

Ключовими елементами у державній системі контролю Internet простору, стеження за його резидентами відбувається в межах проектів «Золотий щит» і «Зелена дамба». На рівні окремої особистості проект «Золотий щит» забезпечує збір інформації, перш за все, в сегменті Internet комунікації за допомогою, так званої, «особистої електронної картки» споживача. В Internet історії Китаю картка виконала і продовжує виконувати надто важливу подвійну функцію: з одного боку вона стала основою системи ідентифікації громадян, що для багатомільйонного Китаю є проблемою «номер один», а з другого — вона стала інструментом збору інформації про всіх користувачів Internet, як це робиться в США і РФ. Контрольну функцію державним органам влади допомагають виконувати й іноземні компанії, які працюють на китайському ринку Internet послуг. Наприклад, на запити влади такі американські фірми як Yahoo, Google і Facebook надають повну інформацію про контент інформацію і розмови всіх «опонентів влади», що явно заперечує інформаційній політиці цих компаній і проголошеним правам людини. Як свідчать експерти на підставі отриманої інформації від цих компаній багато людей були притягнуті до відповідальності за антидержавну діяльність. Такий факт не міг залишитися не поміченим широкою громадськістю Китаю, що призвело до того, що ці компанії зазнали відвертої критики з боку світової Internet спільноти і правозахістних організацій.

Контрольну сторону інформаційної політики Китаю підживлює і контрольоване зростання самої мережі телекомунікацій. Так, станом на 2003 рік у Китаї було побудовано більш ніж 10 мереж, які були зобов'язані надавати уряду інформацію про своїх клієнтів і блокувати контент закордонного походження, який забороненим до використання в країні [10, с. 198–204]. Проект «Зелена дамба», хоча і стосувався програмного забезпечення власного виробництва, яке встановлювалося на комп'ютери іноземного виробництва, але він сприяв тому, що через комп'ютеризацію закладів освіти й Internet кафе уряд взяв під контроль весь потік інформації й осіб, які використовували її у власних цілях [10, с. 197–198].

Така особливість організації контрольно-скринінгової діяльності провідними країнами у національному сегменті кіберпростору і перенос цієї практики за його кордони породжує певні лінії міждержавного протистояння. Вагомим аргументом такого стану можуть слугу-

вати регулярні повідомлення WikiLeaks про шпигунську (і кібертерористичну) діяльність США. Наприклад, у березні 2017 року WikiLeaks оприлюднив більш ніж 8 тис. документів, що стосуються діяльності групи хакерів, які працюють під «дахом» ЦРУ США у Центрі збору інформації, розташованому у Франфуркті-на-Майні (Німеччина). Оприлюднена інформація зачіпає найчутливійше питання функціонування Internet проекту як відкритої і прозорої площадки для всієї міжнародної спільноти. Проблема полягає у використанні інформаційних технологій, про що йшлося вище, у військово-політичних цілях з ворожими намірами. Її коріння знаходиться у трикутнику інформаційних стратегій США, РФ і Китаю. Ключова відмінність між позицією США, з одного боку і позицією РФ і Китаю, з другого боку, корениться у тому, що США та їхні союзники дотримуються точки зору, що на міжнародному рівні слід розглядати лише питання кібербезпеки (техніко-технологічну складову інформаційного простору, іноді її ще називають інструментальною складовою), залишаючи питання інформаційно-психологічних впливів за межами дискусійного поля. Позиція Китаю, РФ і країн, які їх підтримують базується на тому, що за інструментальною складовою завжди присутні приховані інтереси суб'єктів інформаційного простору, які переслідують економічні, політичні, соціальні і воєнні цілі. Звідси, на відмінну від США й їхніх союзників, в контексті можливих домовленостей щодо підходів у розумінні поняття «інформаційного простору», Китай і РФ виступають за визнання у його складових не тільки інструментальної частини, на чому наполягають США, але й суб'єктної, тобто рівності у правах (і відповідальності) всіх резидентів Internet проекту. І хоча на площадці ООН з цього приводу відбуваються досить гострі дебати, досягти результатів поки ще не вдається. Як констатує дослідник цього питання Д. Дубов позиція ООН виглядає «якщо не як компроміс між двома альтернативами, то принайми як таке, що може вести до зазначеного компромісу» [10, с. 160].

4. Висновки

В умовах зростання ризиків і викликів інформаційного середовища та з метою збереження соціально-політичної стабільності, держави прагнутимуть використовувати інформаційні технології у якості латентного інструментарію тотального контролю за приватним життям громадян. Як ресурс політики інформаційної безпеки цей інструментарій дозволяє відслідковувати суспільні тенденції негативного характеру і з позицій національних інтересів своєчасно реагувати на їх прояви. Аналіз типових проявів цієї політики на прикладі США, РФ і Китаю показує тенденцію до активізації ролі інституту держави у цій справі і вивірену лінію поведінки провідних країн на міжнародних площадках щодо рішень у цьому чутливому питанні національної безпеки.

5. Список літератури:

1. Гегель Г. В. Ф. Философия права. — М.: Мысль, 1990. — 524 с.
2. Шкепу М. А. Феноменология истории в трансформациях культуры. — К.: Книжное издательство НАУ, 2005. — 360 с.
3. Лем С. Сумма технологий / С. Лем. — М.: Мир, 1968. — 608 с.
4. Чернов А. Становление глобального информационного общества: проблемы и перспективы//http://www. isn. ru/public/Book. zip.
5. Глобалізація і безпека розвитку: Монографія / Білорус О. Г., Лук'яненко Д. Г. та ін.; керівник авт. колективу і наук. редак. О. Г. Білорус. — К.: КНЕУ, 2001. — 733 с.
6. Юнгер Ф. Г. Совершенство техники. — СПб.: ВЛАДИМИР ДАЛЬ, 2002.- 553 с.
7. Бейлин М. В. Новые технологические угрозы информационной безопасности личности//Час вибору: виклики інформаційної епохи: колективна монографія/за заг. ред. О. А. Івакіна, Д. В. Яковлева. — Одеса: Видавничій дім «Гельветика», 2016. — 472 с

8. Фурашев В. Проект Wikileaks та його сутність // Комуфляж № 2. — 2011.

9. Электронный концлагерь: по етапу идет «Ешелон»// «Русский вестник». — 2003. — № 14. — [Електронный ресурс]. — Режим доступа: http://www. x-libri. ru/elib/smi01405/00000001.html.

10. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія/Д. В. Дубов. — К.: НІСД, 2014. — 328 с.

11. Сулейманов С. Следим строже чем за русскими/ С. Сулейманов [Электронный ресурс]. — Режим доступа: https:// lenta. ru/ articles/2013/06/01/ bigbro/.

12. Пожидаев Е. Инструментарий тотальной слежки и современная система кибершпионажа/ Е. Пожидаев [Электронный ресурс]. — Режим доступа: https:// regnum. ru/ news/1683920 html.

13. Леонов С. Это холодная война? Российским чиновникам запретили пользоваться сервисами Google / С. Леонов [Электронный ресурс]. — Режим доступа: https:// ura. ru/ news/105185439.

14. Ивей Ван. Китайськая модель разрушает гегемонию «общечеловеческих ценностей» [Электронный ресурс]. — Режим доступа: http://inosmi. ru/ world/20130114/204595110.html.

References:

1. Gegel,G.V.F. (1990), Filosofiya prava, Myisl, M, 524 p.

2. Шкепу М. А. Феноменология истории в трансформациях культуры. — К.: Книжное издательство НАУ, 2005. — 360 с.; Shkepu M. A. Fenomenologiya istorii v transformatsiyah kulturyi. — K.: Knizhnoe izdatelstvo NAU, 2005. — 360 s.

3. Lem,S. (1968), Summa tehnologiy, Mir, M, 608 p.

4. Chernov, A. «Stanovlenie globalnogo informatsionnogo obschestva: problemy i perspektivyi», available at: http://www. isn. ru/public/Book. zip. (accessed 16 febriary 2017).

5. Bilorus,O.H., &Lukianenko, D.H. (2001), «Hlobalizatsiia i bezpeka rozvytku», KNEU, K, 733 p.

6. Yunger, F.G. (2002), Sovershenstvo tehniki, VLADIMIR DAL, 553 p.

7. Beylin,M.V. (2016), «Novyie tehnologicheskie ugrozyi informatsionnoy bezopasnosti lichnosti» in Ivakina, O.A., & Yakovleva, D.V., (Eds.), «Chas vyboru: vyklyky informatsiinoi epokhy» Vydavnychii dim «Helvetyka», Odesa, pp..67–78.

8. Furashev, V. (2011), «Proekt Wikileaks ta yoho sutnist», Komufliazh vol. 2, pp. 16–17.

9. RUSSKIY VESTNIK (2003), «Elektronnyiy kontslager: po etapu idyot «Eshelon», available at: http://www. x-libri. ru/elib/smi01405/00000001.html. (accessed 09 april 2017).

10. Dubov, D.V. (2014), «Kiberprostir yak novyi vymir heopolitychnoho supernytstva», NISD, K, 328 p.

11. Suleymanov, S. «Sledim strozhe chem za russkimi», available at: https:// lenta. ru/ articles/2013/06/01/ bigbro/. (accessed 14 febriary 2017).

12. Pozhidaev, E. «Instrumentariy totalnoy slezhki i sovremennaya sistema kibershpionazha», available at: https://regnum. ru/news/1683920 html. (accessed 16 april 2017).

13. Leonov S. «Eto holodnaya voyna? Rossiyskim chinovnikam zapretili polzovatsya servisami Google», available at: https://ura. ru/news/105185439 (accessed 20 april 2017).

14. Ivey Van. «Kitayskaya model razrushaet gegemoniyu «obschechelovecheskih tsennostey», available at: http://inosmi. ru/world/20130114/204595110.html. (accessed 21 febriary 2017).