Розділ

7 ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

7.1. ДО ПИТАННЯ ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Матеріали до проекту рішення РНБО України
"Про заходи щодо вдосконалення державної інформаційної політики
та забезпечення інформаційної безпеки України"
(Київ, НІСД, жовтень 2001 р.). *Публікується вперше.*

Аналіз проблем, що виникають у сфері забезпечення інформаційної безпеки, дає змогу зробити висновок про необхідність удосконалення законодавчої бази в інформаційній сфері.

По-перше, йдеться про розроблення та прийняття Верховною Радою України Закону України "Про свободу доступу до інформації" (на зразок Акта про свободу інформації США). У цьому законі слід передбачити дієві заходи для забезпечення свободи доступу громадян до урядової інформації, презумпції несекретності, обов'язковості регулярного оприлюднення органами державної влади докладних звітів про свою діяльність тощо. Разом з тим необхідно, щоб цей закон передбачав достатнє фінансування згаданих заходів з державного бюджету, адже інакше його прийняття не матиме жодного сенсу.

По-друге, потрібно розробити та прийняти закони, які б визначали статус і режими захисту інформації, що не містить державної таємниці, але належить до інших передбачених законодавством видів таємниці (лікарська, банківська, персональна тощо). Всі проблеми, пов'язані з обмеженням доступу до інформації, мають бути законодавчо врегульовані. Слід значно прискорити розроблення та прийняття Закону України "Про національну систему конфіденційного зв'язку".

По-третє, необхідно удосконалити нормативно-правову базу функціонування галузі зв'язку та телекомунікацій, насамперед прийняти Закон України "Про телекомунікації".

По-четверте, слід розробити та прийняти закони України про політичну пропаганду, політичну рекламу, паблік рилейшнз тощо, які б урегульовували ці складні політичні проблеми.

По-п'яте, потрібно законодавчо регламентувати діяльність інформаційно-аналітичних центрів, насамперед тих, що фінансуються з-за кордону. Разом з тим при формуванні бюджету необхідно передбачити виділення коштів на розвиток інформаційно-аналітичної діяльності, наприклад, через створення фонду аналітичних досліджень, державного сприяння фінансуванню цих досліджень вітчизняними бізнес-структурами.

По-шосте, необхідно внести зміни та доповнення до Закону України "Про телебачення та радіомовлення", Закону України "Про Національну раду України з питань телебачення та радіомовлення" щодо захисту суспільної моралі від засилля культу жорстокості і насильства на телебаченні, в кіно та відеопрокаті.

Значної інтенсифікації потребує діяльність щодо кодифікації інформаційного законодавства і створення Інформаційного кодексу України.

Не менш важливо здійснити комплекс заходів адміністративного характеру. Назріла необхідність перебудови системи державного управління інформаційною сферою. Зокрема, в Україні де-факто немає органу, який би відповідав за розроблення та реалізацію державної інформаційної політики.

Слід негайно створити державну структуру, завдання якої полягатимуть у виробленні та реалізації державної інформаційної політики. Найдоцільніше сформувати цю структуру саме в системі Адміністрації Президента України, у чому, зокрема, переконує і світовий досвід.

Зазначена координаційна структура повинна бути постійно діючим органом державної влади з чітко визначеними функціями, повноваженнями, який буде забезпечений матеріально-фінансовими ресурсами та кадрами, достатніми для вирішення покладених на нього завдань. Водночас, як доводить досвід 10 років незалежності, функціонування колегіальних дорадчих структур, як правило, не зовсім ефективне.

На особливу увагу заслуговують питання чіткої регламентації взаємодії новоутвореної структури з органами виконавчої влади, насамперед з Кабінетом Міністрів України. Важливим напрямом її функціонування має стати координація діяльності центральних і місцевих органів державної влади щодо забезпечення зв'язків із громадськістю та інформаційно-пропагандистської підтримки державних рішень.

Перегляду потребує і чинна нормативна база стосовно функціонування органів виконавчої влади. Зокрема, до Положення про міністерства і відомства мають бути обов'язково внесені пункти щодо необхідності інформування громадськості про діяльність цих структур. Слід встановити чіткі вимоги до представлення органів державної влади в Інтернеті, створення загальнодоступних баз даних, насамперед нормативно-правової інформації. Витрати на цю діяльність мають враховуватися під час підготовки державного бюджету та визначатись у ньому окремо.

Вирішення зазначених питань дасть можливість значно поліпшити ситуацію в інформаційній сфері та підвищить рівень забезпечення інформаційної безпеки України.

7.2. ІНФОРМАЦІЙНА ВІДКРИТІСТЬ ДЕРЖАВНОЇ ВЛАДИ В УКРАЇНІ ЯК ЗАПОРУКА ЇЇ ЕФЕКТИВНОСТІ

Власюк О. С. Виступ на відкритті Міжнародного експертного "круглого столу" "Відкритість та прозорість української влади в умовах її реформування" (Київ, НІПМБ, 30 листопада 2007 р.) *Публікується вперше.*

Інформаційна відкритість і прозорість влади є необхідними передумовами сталого демократичного розвитку суспільства та держави. Лише на таких засадах можливі реальний громадянський контроль і зміцнення довіри громадян до влади.

Україна має достатню законодавчу базу, яка повинна забезпечити безперешкодний доступ громадян до інформації про діяльність органів влади. Проте ситуація з погляду забезпечення відкритості та прозорості влади далека від ідеальної, яку описують різноманітні партійно-урядові програми, часто не відповідаючи сучасним цивілізаційним стандартам у сфері інформаційної відкритості. За це ми платимо дорогою ціною недовіри іноземних партнерів, втратою потенційних інвесторів тощо.

Достатньо фактів, які свідчать, що така констатація не є надуманою. Наприклад, для нас дотепер закрито багато сторінок власної історії; ми не знаємо, наскільки безпечною для проживання є не лише Чорнобильська зона, а й зона будь-якого українського мегаполісу, починаючи з Києва. Унаслідок браку необхідної інформації в Україні можливе існування "еліта-центрів" та процвітання різноманітних рейдерів.

Водночас, мабуть, ні в кого не викликає сумніву, що потрібен розумний баланс між відкритістю і закритістю. З одного боку, він має забезпечити справжню свободу слова та свободу діяльності засобів масової інформації, з іншого – не повинен загрожувати безпеці держави.

Однак трапляються перекоси, пов'язані з надмірним утаємничуванням інформації. Слід зазначити, що Україна успадкувала від колишньої "імперії" потужне прагнення втаємничувати інформацію за принципом "аби чого не трапилось". Сьогодні це підкріплюється також бажанням будувати непрозорі тіньові відносини в багатьох сферах суспільного розвитку, починаючи від економіки, значна частина якої перебуває в "тіні", й закінчуючи освітою та медициною. В сукупності це постійно підживлює і формує соціальну базу для корупції у багатьох її формах та проявах.

Така ідейна й кадрова спадщина дотепер багато в чому визначає не тільки розвиток нормативно-правової бази у сфері захисту державної таємниці, а й психологію та поведінку державних управлінських кадрів, наслідком чого є їх надмірна закритість від суспільства.

Варто нагадати, що прийнятий у 1994 р. Закон України "Про державну таємницю" вивів нашу, колись повністю "засекречену", країну на принципово новий правовий рівень розвитку. Водночас недоліком цього та інших профільних законів є недооцінка питань взаємодії сучасної Української держави з бізнесом та корпоративним сектором економіки, що має негативні наслідки для економічного розвитку країни.

З цього погляду характерною є відсутність надійних законів, які б регулювали й гарантували комерційну та приватну таємницю, а це можна навіть розцінювати як небажання рахуватися з приватними інтересами. Світовий досвід, накопичений у цій сфері, з великими труднощами імплементується в нашій країні.

В Україні постійно звужується коло експертів, причетних до конфіденційної інформації та державної таємниці, а також немає системи ефективного суспільного контролю над цією сферою інформаційної діяльності, насамперед з боку парламенту й незалежних ЗМІ. Унаслідок цього неминучими є різноманітні затримки з цільовим оприлюдненням життєво важливої для соціуму інформації, що виводить її із суспільного обігу з усіма подальшими небажаними економічними, соціальними та політичними наслідками.

Насамкінець варто наголосити, що поняття "відкритість і прозорість влади" не зводяться лише до цивілізованого регулювання відносин політиків та державних службовців з громадянами, хоча це також дуже важливе й наболіле питання. Відкритість української влади – це передусім наявність в Україні тих соціально-політичних інституцій, які є звичними для розвинених західних країн і спроможні забезпечити ефективний громадянський тиск на владу. Лише це може забезпечити потрібну громадянам спрямованість дій влади і сформувати в кінцевому підсумку архітектуру владної системи, дружньої для кожного громадянина зокрема і для громадянського суспільства загалом.

Відкритість влади у такому контексті – це бажання й уміння владних суб'єктів ділитися владою з її об'єктами. У цьому розумінні відкритість – ефективний інструмент забезпечення оптимального зворотного зв'язку, який дає змогу ефективно управляти й будувати діалог між владою та громадянським суспільством.

7.3. СУЧАСНІ ПОЛІТИЧНІ ТЕХНОЛОГІЇ МАНІПУЛЮВАННЯ КОНЦЕПТОМ "УКРАЇНСЬКОГО ПОЛІТИЧНОГО ХАОСУ" В ЗАРУБІЖНИХ ТА ВІТЧИЗНЯНИХ ЗМІ

Власюк О. С., Недбаєвський С. Л. Матеріали до аналітичної довідки (Київ, НІПМБ, серпень 2007 р.). *Публікується вперше.*

Нинішній етап розвитку української державності характеризується посиленням інформаційної боротьби в усіх сферах суспільно-політичного життя. За умов загострення політичного протистояння всередині країни Україна стає об'єктом активних медіа-атак іззовні: як зі сходу, так і з заходу. Цю тенденцію необхідно враховувати під час розроблення стратегії нейтралізації загроз національній безпеці в інформаційній сфері, а також у розбудові іміджу України у світі.

Спільною рисою сучасних маніпулятивних технологій є їх негативізм, спрямованість на формування у користувачів інформаційного продукту негативного ставлення до політичних рішень та їх суб'єктів – владних інститутів, а деколи й до принципу порядку загалом. Надійним індексом, що дає можливість визначити наявність застосування негативістських технологій, є зростання ентропійних тенденцій у суспільстві, утвердження в масовій свідомості настроїв песимізму і занепаду, знецінювання базових морально-етичних суспільних цінностей.

Окремим рядком у низці технологічних засобів маніпуляторів масовою свідомістю стоїть використання метафори "політичного хаосу" як засобу відмови тому чи іншому владному суб'єкту (політичному інституту або державі загалом) у здатності до адекватної реакції на стан справ у суспільстві, а також до ефективного раціонального управління країною.

Така інтенція до знецінювання владного інституту (або держави загалом), а також до втручання у внутрішні справи політичного суб'єкта, що "допускається" з метою "відновлення порушеного порядку", ріднить концепт політичного хаосу з концептом неспроможної держави, який використовується нині для здійснення непрямого ("м'якого") політичного тиску на незговірливе керівництво окремих країн.

У прагненні копіювати новітні розробки США у сфері проведення інформаційно-пропагандистських операцій Росія активно використовує концепт неспроможної держави для реалізації цілей своєї експансіоністської інформаційної політики на пострадянському просторі.

На думку основних розробників цієї теми – експертів впливового американського журналу *Foreign Policy*, а також фахівців дослідницького центру "Фонд за мир" (*Fund for Peace*), що публікують щорічні рейтинги нестабільних держав, – стан політичного хаосу в країні є атрибутом (невід'ємною ознакою) і одночасно похідною (наслідком неправильного функціонування) більшості держав, що наближаються за політико-економічними характеристиками до категорії неспроможних держав. Таким чином, використання щодо тієї або іншої країни терміна "політичний хаос" завжди передбачає приховану або явну вказівку на слабкість, недієздатність, неспроможність політичної влади країни.

Справедливим є і протилежне. Термін "неспроможна (помилкова) держава" неявно вказує на політичну нестабільність і можливість соціально-політичного хаосу. Так, розвиваючи маніпулятивний вплив у ЗМІ за напрямами, окресленими у визначенні "неспроможна держава", деякі суб'єкти інформаційного впливу формують українську і міжнародну суспільну думку в бік сприйняття політичної та соціальної нестабільності в Україні, що нібито зростає, а також перманентної загрози політичного хаосу і, як наслідок, розпаду країни.

Визначення терміна "неспроможна держава" акцентує увагу на таких ключових критеріях недієздатності політичної влади:

– влада не має ефективного контролю над власною територією;

– влада створює штучні перешкоди для економічного розвитку країни та її інтеграції у світову економічну систему;

– влада не сприймається як легітимна значною частиною населення країни;

– влада не забезпечує внутрішньої безпеки і базових прав громадян;

– влада не володіє монополією на використання сили.

Своєрідним тестом схильності ЗМІ до негативістських тенденцій щодо України стали події після оголошення Указу Президента України про розпуск Верховної Ради. Реакція на них різних українських та закордонних ЗМІ визначила, як далеко ті чи інші суб'єкти інформаційного впливу можуть піти у використанні негативістських маніпулятивних технологій.

Більшість російських ЗМІ, коментуючи події в Україні навколо розпуску парламенту, віддавала перевагу негативному (явному або прихованому) висвітленню

дій української влади, а також тенденційним прогнозам щодо наслідків зростання суспільно-політичної активності в країні. Акценти було зроблено на процесах дезінтеграції української влади та деконсолідації українського соціуму. Позитивні тенденції – очищення влади і згуртування значної частини українського суспільства навколо президентських рішень, навпаки, замовчувалися.

Підкреслювалися "неадекватність" і "непослідовность" дій президентської сторони, а також її відповідальність за можливе скочування країни до політичного хаосу. У маніпулятивному розкритті російськими ЗМІ теми неспроможності української влади до ефективного управління інформація подавалася за напрямами, що збігаються з наведеними характеристиками "неспроможної держави".

1. Влада створює штучні перешкоди для розвитку економіки країни та її інтеграції у світову економічну систему.

Поширеними на економічному напрямі російської інформаційної пропаганди є звинувачення української влади (насамперед президентської команди) в упередженому ставленні до Росії та намаганнях якщо не зруйнувати українсько-російську економічну співпрацю, то принаймні загальмувати її розвиток. Наміри російської сторони щодо чергового підвищення ціни на газ для України висвітлюються як реакція на ворожі плани стосовно Росії, що їх начебто розробляють у Секретаріаті Президента України. Будівництво Росією трубопроводів в обхід української території також подається російською стороною як крок у відповідь, тобто як наслідок дій керівництва України (типовий приклад використання технології перекладання відповідальності).

Українській стороні активно нав'язується роль провокатора штучних конфліктів та непорозумінь в економічних відносинах із Росією. Основними технологіями, що використовуються на цьому напрямі, є стереотипізація та гра на забобонах. Роздмухується центральна з часів Помаранчевої революції теза російської пропаганди: "Наша Україна" уособлює прозахідні сили, що негативно ставляться до Росії та бажають завдати їй шкоди". Цей стереотип, що його вже декілька років активно формує російська пропаганда, у вигляді базового підсвідомого припущення міститься у багатьох оцінках російськими ЗМІ дій президентської команди.

Наслідком застосування технології стереотипізації є підміна раціонально-логічних підходів до вирішення політичних проблем емоційним, упередженим ставленням, що унеможливлює спокійний зважений діалог. Стереотипи, які формують російські ЗМІ, відволікають увагу людей від реалій сучасного стану справ в українсько-російських відносинах у площину емоційних оцінок та штампів, щодо яких не треба замислюватися.

Ми змушені констатувати, що сьогодні певна частина українського суспільства сприймає за істину неадекватний пропагандистський штамп стосовно антиросійськості демократичних пропрезидентських сил в Україні. Тому подолання цього стереотипу та його пропагандистського неукраїнського коріння має відбуватися на всіх рівнях вітчизняної інформаційної роботи.

2. Влада не сприймається як легітимна значною частиною населення.

Цю тезу, прямо чи як підсвідоме припущення, містила більшість коментарів російських ЗМІ щодо масових соціальних заворушень, які відбулися після підписання квітневого Указу Президента України про розпуск Верховної Ради України.

У політичній аналітиці тих подій на шпальтах багатьох російських видань Президент України поставав як такий, що "зламав встановлені правила політичної гри" та здатний і надалі перекроювати ці правила доти, доки не нав'яже свою волю політичним опонентам і всьому українському народові. Президентові приписувались такі якості, як непередбачуваність та схильність до авторитарних дій.

Серед прийомів маніпулювання масовою свідомістю, що домінували на цьому напрямі російської пропаганди, можна виокремити:

– замовчування справжніх причин (а саме політичної корупції у Верховній Раді), що призвели до президентського рішення;

– напівправда – однобоке висвітлення подій тільки з позицій членів коаліції та їх прихильників;

– карикатуризація дій Президента України, підміна його справжніх державницьких мотивів та щирої стурбованості долею країни егоїстичними мотивами збереження влади;

– використання образливих звинувачень і порівнянь (порівняння з Б. Єльциним, Л. Кучмою, звинувачення в авторитарних нахилах тощо).

Але головною технологією, використаною на цьому етапі, була десакралізація – різновид постмодерністської деконструкції ідей. Сутність її полягає в тому, що під прикриттям показної стурбованості процесом руйнування авторитету законодавчої та судової гілок влади вчиняються дії, спрямовані на тотальне знецінювання й делегітимізацію у свідомості населення дій та рішень саме Президента України і його Секретаріату.

Основними психологічними прийомами, що використовувалися російськими ЗМІ на напрямі делегітимізації та десакралізації української влади, були такі:

– протиставлення Президента України народові;

– роздмухування параноїдального страху: президент та його оточення замислили завдати шкоди Україні;

– безапеляційні заяви, що подаються як факт ("масові порушення законів та Конституції в Україні стали звичайною справою");

– натяк на ірраціональність мотивів та імпульсивність дій президента ("президенту не подобається чинне законодавство, тому він вирішив його скасувати");

– використання різких висловлювань ("жорстке протистояння", "війна на знищення");

– демонстрація позиції активного захисника інтересів пересічного українця;

– багаторазове повторення одних і тих самих тез та висловлювань для закріплення стереотипів;

– підкидання у масову свідомість негативних сценаріїв, що здатні самореалізовуватися, та нагнітання катастрофних настроїв.

3. Влада не забезпечує безпеки і дотримання основних прав громадян та не володіє монополією на використання сили.

Розвиваючи цей напрям інформаційної експансії на українському інформаційному просторі, російські ЗМІ зосередилися на тенденційному висвітленні ситуації, яка склалася щодо критики діяльності деяких суддів Конституційного Суду України з боку Секретаріату Президента України; подій навколо відставки Генерального прокурора України та перепідпорядкування підрозділів внутрішніх військ МВС України Президентові.

Водночас у російських ЗМІ мусувалися такі основні теми:

– безправності в умовах розвалу судової системи українських громадян (навіть суддів Конституційного Суду України) перед "свавіллям" Секретаріату Президента;

– смакування можливості та наслідків фізичного протистояння людей на вулицях;

– подання ситуації у безпековій сфері України як неконтрольованої внаслідок розколу силових структур на підрозділи, лояльні до Президента України, та ті, що підтримують В. Януковича;

– тенденційне висвітлення непослідовності та незграбності дій українських посадовців, насамперед Секретаріату та Служби охорони Президента України, що буцімто тільки посилювали владний хаос.

В інформаційний простір були вкинуті фрази "державний заколот", "передчуття громадянської війни", "протистояння силовиків", "можливий розстріл парламенту" та ін.

Основною технологією, що мала б тримати людей у напруженні, стало роздмухування міфів про наміри запровадити в Україні надзвичайний стан, які нібито були в Секретаріаті Президента України, та про велику ймовірність (запрограмованість) повторення Україною російського досвіду 1993 р. З цією метою повідомлення з України на початку більшості інформаційних випусків виходили безперервно, як із зони бойових дій (так званий воєнний телеграфний стиль). Диктори телебачення мали стурбований вигляд та тривожну тональність у голосі.

Водночас застосовувалися такі прийоми маніпулятивного впливу:

– посилення висловлювань за рахунок акцентів;

– оперування історичними матеріалами для підкреслювання значущості та масштабності подій;

– формування ілюзії незалежного вибору: висвітлення у кількох інтерв'ю різних позицій, але з таким розрахунком, щоб виставити у вигідному ракурсі лише одну необхідну;

– домінування негативних повідомлень про Україну над позитивними.

Отже, можна зробити висновок, що російська пропаганда щодо України стає дедалі більш цільовою, активною й агресивною та застосовує на українському інформаційному просторі широкий арсенал пропагандистських засобів та маніпулятивних технологій.

Досить чітко останнім часом окреслилися дві тенденції, характерні для російської інформаційної політики стосовно України: тенденція імітування західної позиції нейтральності щодо внутрішньополітичного становища в Україні, а також тенденція до знецінювання Української держави під загальним знаменником розглянутого вище концепту "неспроможної держави".

В основу практики пропагандистської роботи покладені концептуалізація і позиціювання. Саме цей ключовий напрям робіт для російських та зорієнтованих на Росію ЗМІ в Україні реалізується, до того ж непогано, московськими аналітиками. Завданням "позиціоністів", відповідно, залишається тільки "обігравати" "концептуальні" ідеї кремлівських політтехнологів "на місцевих прикладах" і транслювати їх на масову українську аудиторію. Саме на цій

первісній позиціонуючій ділянці пропаганди позначається концептуальний "голод" національно орієнтованих українських ЗМІ, який слід якнайшвидше подолати за рахунок створення ефективних національних аналітичних центрів.

Західні коментатори також активно використовують концепт "українського політичного хаосу", щоб зі свого боку висловити незадоволення розвитком подій в Україні і так "навернути" українське керівництво на "шлях істини". Аналіз західної преси демонструє "моду" на розчарування Україною, що останнім часом утверджується в західному політичному дискурсі. Тональність розчарування Президентом України домінує в американській, британській, німецькій, французькій, польській пресі та окремих публікаціях в інших європейських країнах.

Це небезпечна тенденція, яку необхідно якнайшвидше проаналізувати та зламати зусиллями вітчизняних політиків, дипломатів, вчених-гуманітаріїв і працівників інформаційної сфери. Адже конструктивна критика та дружня стурбованість долею партнера на шляху до демократії, природні для відносин сучасної (післяреволюційної) України і Заходу, в умовах інформаційного протистояння у світі, що зростає, можуть бути штучно перетворені на взаємне непорозуміння та знецінювання, що вже активно використовують вороги української демократії як усередині країни, так і ззовні. У результаті необачної політики Європи і США стосовно України наша держава знову може стати "розмінною монетою" у геополітичних іграх Росії та Заходу і сплатити за це новими втратами іміджу. Тому треба невтомно роз'яснювати західним партнерам складність та масштабність завдань, які стоять перед молодою українською демократією на її шляху до євроатлантичної спільноти, важливість консолідованих зусиль світових демократій з підтримки європейського курсу України, а також безальтернативність цього курсу для нашої країни.

Високий рівень негативного ставлення в західній пресі спостерігається стосовно як Президента України, так і парламентсько-урядової коаліції. Наявність таких критичних повідомлень свідчить про виникнення сумнівів серед політичної еліти Заходу щодо ефективності українського політикуму.

Деякі західні ЗМІ схильні підпадати під навіювання оманливої логіки російських геополітичних міфів, розглядаючи Україну не як суб'єкт, а як об'єкт міжнародних відносин у великій геополітичній грі. Знову-таки під прикриттям базового припущення про неспроможність української влади до консолідації виголошується дуже небезпечна теза про природність регіональних відмінностей та теоретичну допустимість розколу держави.

Отже, у реакції західних ЗМІ на українські події квітня – червня 2007 р. ми бачимо дві небезпечні тенденції: демонстративне розчарування діями української влади та схильність "грати" з небезпечними геополітичними конструктами, відпрацьованими кремлівськими політтехнологами, сприймаючи ці конструкти майже як реальність.

Підсумовуючи викладене, слід зазначити таке.

1. У результаті викривленого подання подій навколо розпуску Верховної Ради деякими зарубіжними масмедіа, насамперед російськими, іміджу української держави було завдано шкоди, як на міжнародній арені, так і всередині країни.

Цю шкоду необхідно якнайшвидше компенсувати за рахунок злагоджених дій державних органів усіх рівнів, причетних до інформаційної сфери діяльності. У цьому напрямі потрібно активізувати зусилля, спрямовані на впровадження розробленої Міністерством закордонних справ України Державної програми формування позитивного міжнародного іміджу України на 2007–2010 роки. На найближчу перспективу слід розробити і реалізувати План невідкладних заходів з підтримки міжнародного іміджу України.

2. Наша держава останніми роками зробила великий крок у бік розширення свободи слова, скасування всіх форм цензури. Це досягнення має зворотний бік у вигляді збільшення вразливості національного інформаційного простору до сучасних прихованих форм маніпулювання масовою свідомістю. Тому сьогодні в Україні є об'єктивна потреба у формуванні громадського інституту контролю за діяльністю масмедіа, який би з-поміж інших питань здійснював незалежне експертне оцінювання маніпулятивних впливів іноземних ЗМІ на українську аудиторію та пропонував заходи щодо їх нейтралізації. З метою створення й активізації такого громадського інституту Національній комісії з утвердження свободи слова та розвитку інформаційної галузі при Президентові України доцільно ініціювати роботу постійно діючого Форуму громадських наглядових рад при провідних теле- і радіоканалах та інших впливових масмедіа, на якому могли б обговорюватися питання захисту національного інформаційного простору України.

3. У психологічному аспекті основну загрозу національному інформаційному простору містять маніпулятивні пропагандистські конструкти, створені навколо історичних і геополітичних міфів, що їх виробляють кремлівські аналітики. З технологічного погляду ці конструкти (або позиціювання) бездоганні. Тому насамперед необхідно подбати про аналітичне забезпечення вітчизняних медіа власним концептуально-ідеологічним продуктом, що міг би на рівних протистояти російському в концептуальній площині. З огляду на ці міркування, доцільно сформувати спеціальну аналітичну групу (інтелектуальний центр), завданнями якої будуть питання концептуального забезпечення національних ЗМІ якісною аналітичною продукцією щодо позиціювання України у світі.

4. Як доводить російський та західний досвід, однією з найефективніших установок при проведенні державного брендингу є висвітлення позитивних моментів. Якщо підрахувати відсоткове співвідношення подання негативних і позитивних фактів про Росію в тамтешніх ЗМІ, воно ніколи не перевищуватиме співвідношення 1:3. Це свідчить про наявність узгодженої позиції серед керівників російських ЗМІ надавати перевагу позитивним фактам і тлумаченням під час висвітлення подій у їх країні, що загалом привело до позитивних результатів. Україні теж варто врахувати цей досвід.

7.4. ПРОБЛЕМИ ДІЯЛЬНОСТІ НЕЗАЛЕЖНИХ АНАЛІТИЧНИХ ЦЕНТРІВ В УКРАЇНІ

Власюк О. С. Виступ на фаховій дискусії "Неурядові аналітичні центри України": новий етап розвитку чи "біг по колу"?" (Київ, Укр. центр екон. і політ. досліджень ім. О. Разумкова, 21 вересня 2007 р.).
Публікується вперше.

За нинішніх українських реалій аналітичні центри (як урядові, так і неурядові) передусім виконують комунікативну функцію. Інакше кажучи, вони є, як уже зазначили організатори дискусії, "інтелектуальними містками", як між владою і суспільством, так і між окремими гілками влади. Звідси випливає висновок: оскільки влада в Україні сьогодні розбалансована і неконсолідована, то певну відповідальність за це мали б узяти на себе вітчизняні аналітичні центри – вони не виконали своєї основної функції і не впоралися з визначеною роллю.

Є теза, згідно з якою значущість мозкових центрів зростатиме в міру інтелектуалізації влади та владних рішень. Але поки що рівень затребуваності різноманітної аналітики в процесі ухвалення рішень низький, і, як наслідок, відбувається їх деінтелектуалізація. Звідси й виникає той невтішний стан, коли рішення в Україні не приймаються, а "трапляються". Зрозуміло, це зумовлює зниження реальних впливів аналітичних центрів на державне й суспільне життя.

Інститут так званої інтелектуальної, або експертної, влади в українському соціумі поки що не склався або не відбувся. Причому на рівні не лише держави, а й недержавних структур. Очевидно, що так триватиме доти, доки заробляти гроші або влаштовувати якісь інші справи у вітчизняному соціумі буде однаково легко як з інтелектом, так і без нього, оскільки саме без особливого напруження думки поки що вирішуються справи у нашому малорозвиненому з ринкової точки зору українському соціумі, хоч і є певні зрушення в його перетворенні на "суспільство знань".

Втішає те, що і владні структури, і різні політичні сили починають розуміти, що без активного втручання в політичні ситуації інтелектуалів та експертів будь-які рішення "зависатимуть" через їх неналежну легітимність і неефективні канали комунікації та імплементації.

Це особливо окреслюється в теперішній ситуації, коли політичні комунікації в Україні опинилися у стані глибокої кризи, що виразно засвідчує нинішня парламентська виборча кампанія. Зважаючи на неї, діяльність українських недержавних аналітичних центрів саме як центрів інтелектуальних сил різко послабилася. Сьогодні вони дедалі більше втрачають арбітражні функції і перетворюються на політико-технологічні установи або тіньові виборчі штаби.

Проблема взаємодії аналітичних центрів з органами влади є досить складною й комплексною. На користь зазначених центрів можна сказати те, що саме вони стали певним стримувальним та комунікативним чинником, який дає громадськості можливість вказувати державним органам на їхні помилки і так опосередковано контролювати їх діяльність. Водночас за умов співпраці, на яку іноді йдуть органи влади в кризових ситуаціях, аналітичні центри спроможні ефективно допомогти в ухваленні важливих стратегічних рішень. Вони

не обтяжені бюрократичними процедурами і можуть залучати неординарних людей, чиї погляди на одну й ту саму проблему під різними кутами зору дають змогу уникати волюнтаристських рішень.

Західний досвід участі аналітичних центрів в ухваленні владних рішень досить багатий. Можемо згадати корпорацію *RAND*, Американський інститут підприємництва (*American Enterprise Institute*), Раду з міжнародних відносин (*Council on Foreign Relations*), Центр Карнегі та інші "фабрики думки", які вже давно і плідно співпрацюють з урядами своїх країн з метою наукової та експертної підтримки стратегічних рішень. Тут ключовим є питання інтегрованості в ухваленні управлінських рішень, що якраз і вимагає від "фабрики думки" незалежного статусу, який нібито гарантує її об'єктивність. Цій тезі суперечить, щоправда, досвід діяльності аналітичних центрів при різних партіях та лобістських угрупованнях. Наприклад, Американський інститут підприємництва завжди працював на ідеологію неоконсерватизму, на Республіканську партію, тоді як Рада з міжнародних відносин традиційно пов'язана з американською Демократичною партією.

Українські реалії засвідчують ту саму тенденцію до партійної ангажованості і значної заполітизованості аналітичних центрів. Ознайомлюючись із їхніми аналітичними продуктами, іноді важко позбутися відчуття, що в них реальне життя підмінене аналітичними витворами, що ґрунтуються на партійно ангажованому баченні устрою світу.

Якщо стисло схарактеризувати ставлення державних структур до аналітичних центрів, то передусім варто назвати недовіру до результатів, отриманих ними. Іноді ця недовіра безпідставна, але часто базується на цілком реальних фактах. Зокрема, коли йдеться про згадану партійну ангажованість або про незрозумілі джерела фінансування досліджень. Важко, скажімо, гарантувати об'єктивність дослідження, якщо воно проводиться за рахунок грантів, які надають представництва іноземних держав або структури, які у нас "модно" називати олігархічними.

Отже, логіку влади в цьому сенсі зрозуміти можна: владні структури або політики, що самі часто фінансують різноманітні псевдогромадські організації, діяльність яких спрямована лише на обслуговування інтересів їхнього основного донора, вважають так само "купленими" всі інші подібні організації. У Росії, як відомо, усі аналітичні центри "третього сектору", що фінансуються з неросійських джерел, почали на офіційному рівні підозрювати в тому, що вони є "елементами широкої мережі зовнішнього тиску".

Цікаво, що найбільшу недовіру у владних структур викликають саме ті продукти аналітичної діяльності, які можуть стати реальним підґрунтям для ухвалення рішень. Ідеться, зокрема, про результати соціологічних досліджень. Вітчизняну соціологію останнім часом часто піддавали жорсткій критиці за її "продажність". Разом з тим, хоча відкидати сам факт наявності "замовлених" соціологічних досліджень не можна, довіра населення до соціології як науки залишається досить високою.

Розглянемо також можливі шляхи зміцнення взаємодії владних інституцій і недержавних аналітичних центрів. Найбільш апробованою та ефективною видається тісніша взаємодія державних і недержавних центрів. Зокрема,

координаційну чи посередницьку роль могли б відіграти аналітичні структури РНБО України та Секретаріату Президента України. Може йтися про спільне написання документів стратегічного значення на зразок традиційних Послань Президента України Верховній Раді України, створення постійно діючих експертних груп, до складу яких входили б представники експертного співтовариства з боку як держави, так і недержавних структур. Необхідно також істотно розширити географічне представництво української аналітики й так само організацій-донорів. Це не зняло б спекулятивні розмови на тему ангажованості аналітичного продукту, але принаймні істотно їх послабило.

Варто також згадати ще одну технологію посилення впливовості аналітичних центрів, яку стабільно демонструє Центр Разумкова. Він досить стабільно делегує своїх експертів до влади, очевидно, сподіваючись, що вони, завершивши цикл владних повноважень, повернуться до Центру, підсиливши його авторитет як аналітичної установи. Саме так, за принципом "сполучених посудин", працюють впливові американські та європейські аналітичні центри, і будемо сподіватися, що цей досвід здобуде визнання і поширеться в Україні. Тоді з трьох альтернатив щодо майбутнього аналітичних центрів України, які сформулювали організатори нинішньої дискусії, дві останні (одержавлення та маргіналізація) можна буде відкинути.

7.5. НАЙБІЛЬШИМ НЕДОЛІКОМ У СПІВПРАЦІ ДЕРЖАВНИХ І НЕДЕРЖАВНИХ АНАЛІТИЧНИХ ЦЕНТРІВ Є СИТУАТИВНІСТЬ

Публікується за: *Власюк О. С.* Найбільшим недоліком у співпраці державних і недержавних аналітичних центрів є ситуативність / О. С. Власюк // Національна безпека і оборона. – 2007. – № 6 (90). – С. 48–49.

1. Чи вважаєте Ви співпрацю органів державної влади з неурядовими аналітичними центрами корисною? Якщо так, то які заходи з боку держави і з боку неурядових аналітичних центрів, на Ваш погляд, мають бути здійснені, щоб зробити таку співпрацю більш ефективною?

У корисності такої співпраці немає жодних сумнівів, оскільки чим інтелектуальнішим буде процес ухвалення рішень, тим більш реалістичними, виваженими, наближеними до життя та перспективними у плані їх імплементації будуть ці рішення.

Інша річ, що у нас ще спрацьовує, на жаль, стара радянська традиція, коли рішення не приймаються, а "трапляються". І тоді аналітиків просять "заднім числом" обґрунтувати ухвалені рішення, надати їм інтелектуальної легітимації. Йдеться, звичайно, про тінізацію політики, її непрозорість і закритість. У такій системі здійснення влади аналітичним центрам робити нічого. Вони у кращому разі виконують лише декоративну функцію.

Узагалі традиція залучати аналітичні центри до процесів формування державної політики має суто американське походження й недостатньо вкоренилася навіть у країнах Західної Європи, де, образно кажучи, немає своїх "РЕНДів" (виняток становить хіба що Велика Британія).

Щодо України, то у нас поки що відбувається суто екстенсивне прирощування кількості аналітичних центрів, але, здається, за рахунок якості праці. Відверто кажучи, до впливу цих центрів на процеси ухвалення рішень зазвичай справа не доходить. У кращому разі вони виконують суто демонстраційні, представницькі ролі, відпрацьовуючи різноманітні гранти іноземного походження. Винятком є хіба що дослідження електоральних уподобань, особливо напередодні виборів, коли до думки неурядових аналітиків уважно прислуховуються масмедіа, а отже, і політики.

Заходи, спрямовані на зближення аналітичних центрів із центрами ухвалення рішень в Українській державі, мають зводитися до тісної професійної взаємодії на рівні експертів. Це передусім формування спільних робочих (експертних) груп із вивчення та розроблення пропозицій щодо вирішення актуальних проблем суспільного розвитку, а також залучення до державного управління фахових аналітиків. Тут маємо позитивний приклад Міністерства оборони, нинішнє керівництво яким успішно працювало свого часу і в Центрі Разумкова, і в аналітичній групі РНБО України. Але важливо, щоб процес рухався і у зворотний бік, тобто керівники високого рівня на той час, поки вони з різних причин не задіяні у владних структурах, тісно співпрацювали з неурядовими аналітичними центрами.

2. Як би Ви оцінили результати співпраці очолюваного вами Інституту з неурядовими аналітичними центрами? Які форми такої співпраці виявилися найбільш ефективними?

В Україні є декілька державних аналітичних центрів, до яких належать і ті два, до керівництва якими я безпосередньо причетний у недавньому минулому й нині, – Національний інститут стратегічних досліджень та Національний інститут проблем міжнародної безпеки.

Основна мета цих установ – підготовка аналітичних матеріалів, які можуть бути корисними для наукового супроводу рішень Президента України та РНБО України. Досягти цієї мети неможливо без тісної співпраці з недержавними аналітичними центрами. Форм такої співпраці чимало, починаючи від спільних представницьких заходів та наукових форумів і закінчуючи спільною роботою в експертних радах та групах у процесі підготовки різних рішень і документів. Це, зокрема, Послання Президента України до Верховної Ради України, Стратегія національної безпеки та чимало інших документів стратегічного значення.

Після того як у структурі РНБО України з'явилася Наукова рада, співпраця між державними й недержавними консультативно-експертними установами має істотно пожвавитися, тому що в принципі йдеться не про те, яким аналітичним центрам віддавати перевагу, а лише про кінцевий результат.

Недостатня стимулююча та координуюча роль держави у співробітництві з громадськими організаціями загалом і науково-аналітичними зокрема в кінцевому підсумку має наслідком нерозвиненість горизонтальних зв'язків між громадськими та державними організаціями, унаслідок чого кожна з них займає окрему нішу і є практично самодостатньою. Є також проблема законодавчого регулювання механізмів взаємодії громадських організацій з державними інституціями.

Не секрет, що перевагою недержавних центрів є їхня гнучка політика щодо добору кадрів під конкретні завдання, можливість залучати на стислий період

креативних фахівців для різноманітних "мозкових штурмів". Але відомо, що переваги є продовженням недоліків. У цьому випадку недоліком недержавних центрів є плинність творчих колективів, які, виконавши конкретне завдання, розпадаються, тоді як у державних аналітичних центрах можна зустріти людей, які роками відстежують динаміку розвитку одних і тих самих проблем, послідовно відточуючи свій професійний рівень.

Найбільшим недоліком у співпраці державних і недержавних аналітичних центрів є ситуативність, відсутність спільних довгострокових проектів, що негативно відображається на результативності. Ще одним недоліком є певна асиметрія інформаційного обміну між зазначеними центрами. Справа у тому, що державні аналітичні центри надають більше інформації для відкритого доступу, ніж недержавні. Йдеться, зокрема, про поточну аналітику, матеріали "круглих столів", конференцій тощо. Проте, мабуть, не варто звинувачувати в цьому фахівців із недержавних центрів, які розцінюють свої результати як інтелектуальну власність, що надає їм певні переваги в ринкових умовах конкуренції.

Отже, для поліпшення співпраці державних аналітичних центрів із недержавними (неурядовими) необхідно практику спорадичного ситуативного співробітництва перетворити на практику постійної координації та стратегічної взаємодії.

7.6. ВЛАДА БЕЗ АНАЛІТИКИ СЛІПА, АНАЛІТИКА БЕЗ ВЛАДИ БЕЗСИЛА

Власюк О. С. Неопубліковане інтерв'ю
(Київ, НІПМБ, червень 2007 р.). *Публікується вперше.*

– Олександре Степановичу, впродовж півтора десятка років Ви знаходитеся біля керма провідних державних аналітичних центрів України. Як перший заступник директора Ви керували науковою діяльністю Національного інституту стратегічних досліджень при Президентові України. З березня цього року Ви є директором Національного інституту проблем міжнародної безпеки при РНБО України. Обидві установи є досить незвичними, оскільки їхні працівники є водночас і науковцями, і державними службовцями. У цьому контексті напрошується запитання: якими Вам бачаться, з позицій свого наукового досвіду, спілкування з владою, роль та значущість у нашій державі різноманітних аналітичних центрів?

– Ваше запитання можна звести до одного спільного знаменника. Фактично у ньому йдеться про наявність в українському соціумі інституту інтелектуальної, або експертної, влади як неодмінної ознаки розвиненої демократії. Адже є пряма й беззаперечна пропорція: чим демократичнішою є країна, тим більше влада в цій країні на всіх її щаблях та всіх її різновидах зважає на думку інтелектуалів та експертів. Якщо в США або країнах Європейського Союзу нікого не здивуєш сотнями і навіть тисячами експертних та аналітичних центрів на зразок знаменитої *RAND corporation*, до яких влада звертається в пошуку правильних рішень, то в українському соціумі інститут інтелектуально-експертної влади лише починає утверджуватися.

– Якою Вам уявляється оптимальна модель наукового супроводу влади, і на яких засадах створюються і мають створюватися вітчизняні RAND corporation?

– Якщо на Ваше запитання відповідати по-чеховськи, пам'ятаючи, що стисліcть – сестра таланту, то варто підкреслити, що сучасні аналітичні центри створюються під потреби політичної практики, на яких засновувався свого часу в США у післявоєнний період *RAND* як американський прототип "фабрики думки". На відміну від звичайних наукових установ, де виробляється принципово нове знання, тут не так уже й важливо, наскільки це знання є новим. Важливим є сам процес тісного поєднання науково-аналітичних досліджень із процесом ухвалення рішень. Абревіатура *RAND*, до речі, це дуже гарно передає, бо є абревіатурою від англійських слів *research* (дослідження) і *development* (впровадження).

Стосовно України, то тут, якщо відповідати на запитання про засади науково-аналітичної діяльності неупереджено, вельми істотним є вплив суб'єктивного чинника, тобто персоналій президентів, прем'єр-міністрів тощо. Скажімо, для Леоніда Кравчука на самому початку української незалежності аналітичні центри уявлялися аксіоматичною потребою для її виживання. У молодої держави на той час було обмаль інтелектуальних ресурсів для формування самостійної зовнішньої політики. Тому йшлося передусім не про внутрішню політику, а про супровід зовнішньополітичної стратегії. Слід згадати, що вся структура наукового супроводу подібних рішень влади залишилася в столиці колишньої держави – у Москві.

Не буду називати цих численних наукових установ із "московською пропискою". Як у таких випадках кажуть – "ім'я їм – легіон". У цьому довжелезному переліку – Інститут сходознавства, який було створено ще в позаминулому столітті, Інститут світової економіки та міжнародних відносин, Інститут США та Канади тощо. Подібних центрів із суто практичною зовнішньополітичною спрямованістю у Києві на той час не було, а ті, що були, виконували набагато скромніші функції, – суто презентаційні.

– Отже, як воно було насправді, біля витоків української державної аналітики?

– Було і просто, і складно водночас. Коли в 1992 р. президент НАН України Борис Патон під час одного з візитів до Леоніда Кравчука розповів про Інститут стратегічних досліджень, щойно створений у структурі Академії, то цей Інститут разом із його тематикою та науковцями відразу потрапив у поле зору президента держави і згодом отримав назву Національного інституту стратегічних досліджень при Президентові України.

Ще через п'ять років, у 1997 р., перший директор цього "стратегічного інституту" академік Сергій Пирожков, який є нині послом України до Молдови, переконав Президента України Леоніда Кучму разом із тодішнім Секретарем РНБОУ Володимиром Горбуліним у необхідності трансформації академічного Інституту Росії в неакадемічний Національний інститут українсько-російських відносин при РНБОУ. Не забуваймо, що в тому таки 1997 р. було підписано Великий Договір із Росією, і відпало засадниче питання, чи визнає Росія нашу українську

незалежність. Віднині постала низка практичних потреб, починаючи від умов базування у Севастополі Чорноморського флоту РФ і делімітації та демаркації кордону й закінчуючи питаннями енергетичної та енерготранзитної безпеки, які потребували й потребують глибокого науково-аналітичного осмислення.

З березня 2001 р. наш інститут ще раз було трансформовано в Національний інститут проблем міжнародної безпеки. Сталося це, знову-таки, під тиском практичних обставин, оскільки питання міжнародної безпеки у світі, який глобалізується, істотною мірою визначають питання національної безпеки. Особливо враховуючи той беззаперечний і доведений усіма міжнародними рейтингами факт, що за показниками політичної, економічної, персональної та технологічної глобалізації наша країна посідає одне з провідних місць у світі. Отже, як би комусь не хотілося відгородити Україну високим парканом від світу, переповненого всілякими викликами, ризиками та загрозами, такі сподівання слід визнати безнадійними, нічим не обґрунтованими утопіями.

Щодо впливових українських "РЕНДів", як державних, так і недержавних "фабрик владної думки", з якими влада реально рахується, то їх число вимірюється поки що двома-трьома десятками. А, якщо говорити про аналітичні центри "першої величини", в яких аналітики працюють не від виборів до виборів, а так би мовити, на постійній основі, то взагалі йтиметься про лічені одиниці. Це, по-перше, ті два центри, які я щойно називав і до яких особисто причетний.

Можу додати ще порівняно новий Інститут національної безпеки, керований колишнім Секретарем РНБО України Володимиром Горбуліним, і декілька високоспеціалізованих державних центрів, науково-аналітичний продукт яких зазвичай позначений реквізитами таємності або конфіденційності, широкій публіці практично не відомий. Зрештою, є ще декілька недержавних аналітичних центрів, продукт яких не маркується грифами секретності, а навпаки – загальновідомий уже хоча б тому, що керівники цих центрів постійно присутні в телерадіоефірі і на шпальтах різноманітних часописів.

Не буду називати ці загальновідомі й "розкручені" у масмедіа прізвища, оскільки не хочеться когось образити неувагою. Щодо самого зв'язку аналітиків із масмедіа, то в цьому немає нічого поганого. Це теж своєрідний спосіб впливати на ухвалення рішень через важелі масових комунікацій.

– Давайте поговоримо про важелі немасових комунікацій. Адже відомо, що в західній традиції аналітичні центри вважаються виняткова важливими інтелектуальними містками між владою й суспільством, між окремими гілками влади, а також між владою формальною і неформальною. Можливо, та криза політичних комунікацій, яку нині маємо в нашій країні і яка вже набула вимірів перманентності, саме тому й виникла, що вітчизняні аналітичні центри є недостатньо впливовими та не виконують повною мірою свої комунікативні функції?

– Що ж, даруйте, але Ваше запитання належить до так званих риторичних, тобто містить у собі майже готову відповідь. "Маємо те, що маємо", тобто ту незрозумілість і непослідовність у діях і вчинках усіх без винятку гілок влади, невміння чи небажання представників різних гілок влади домовлятися заради спільного добра й досягнення спільного результату. Значною мірою це

є наслідком того, що політики в боротьбі за владу нерідко заходять так далеко, що перестають зважати не лише на опонентів, а й навіть на експертів та власних радників.

Отже, лише всерйоз і надовго подружившись з інтелектуалами й експертами, влада зможе бути переконливою як для власного народу, так і для світової громадськості. Така влада частіше вигравatиме, ніж програватиме у внутрішньому та зовнішньому інформаційному просторі, а отже, сприйматиметься як влада передбачувана, яка хоче і вміє уважно прислухатися до думки експертів, аналітиків. Тобто це важливо для самого внутрішнього та зовнішнього іміджу влади. Не забуваймо, зрештою, що ми живемо в епоху глобалізації, інформаційної революції та інтелектуальної економіки.

– Чи можна з Ваших слів зробити висновок, що значущість "фабрик владної думки", подібних до очолюваного Вами інституту, зростатиме в міру того, як зростатиме інтелектуальний рівень влади?

– Саме так, і не інакше. В ідеалі я та мої колеги вітали б такий стан справ, коли авторитетні люди з владних кабінетів переходили б на постійній або тимчасовій основі на роботу до науково-аналітичних установ. Це як у пролетарського поета колись було написано про селян, які буцімто "трошки орють землю, а трошки пишуть вірші".

Політик і аналітик – це, звичайно, дуже різні за складом характеру люди. Один схильний до негайного реагування, а інший – до тривалої рефлексії. Саме тому вони й доповнюють один одного. Бувають також, дякувати Богу, приємні винятки, коли риси реактивного та рефлексивного характеру поєднуються в одній людині, й тоді вона, попрацювавши певний час в аналітичній установі, разом зі своєю політичною силою, якщо ця сила переможе на виборах, повертається до виконання владних повноважень. Зрештою, як і навпаки.

Одним із нечисленних у наших українських реаліях прикладом такої людини з практичним та водночас аналітичним складом характеру є Володимир Горбулін. До таких людей я відношу і своїх колишніх директорів, з якими разом пройшов шлях становлення Національного інституту стратегічних досліджень, – Сергія Пирожкова та Олександра Бєлова. Але якщо для нас це все-таки не правило, а своєрідна політична екзотика, то в країнах демократично розвиненого Заходу це рутинна практика. Політично впливові люди там не роблять трагедії з того, що певний час їм доведеться працювати не в режимі політичного реагування, а в режимі аналітичної рефлексії. Саме звідси й народжується високий авторитет аналітичної та експертної діяльності.

Відрадним є той факт, що українські політики нової генерації дедалі частіше починають розуміти, що без активного втручання інтелектуалів та експертів у політичні ситуації будь-які рішення, навіть наймудріші, "зависатимуть", хоча б унаслідок неналежної легітимації й неефективних каналів комунікації та імплементації. Це розуміння стає особливо очевидним у нинішній ситуації, коли політичні комунікації в Україні підійшли до небезпечної кризової межі.

Зауважу насамкінець, що поки в нашому соціумі заробляти гроші або влаштовувати якісь "оборудки" буде однаково легко, що з інтелектом, що без нього, будь-які аналітичні центри вважатимуться або непотрібними, або потрібними

лише з точки зору іміджу, незалежно від того, якими вони є, ці центри, – державними чи недержавними. Отже, сам по собі той факт, що в системі української влади є зо два десятки експертних та аналітичних установ, свідчить на користь цієї влади.

– Що Ви могли би сказати про діяльність українських недержавних аналітичних центрів та їх взаємодію з державними?

– Проблем у цих центрів у процесі їх взаємодії з органами влади справді вистачає, і ці проблеми є вельми складними та комплексними. Абстрагуючись від конкретних прикладів і реалій сьогодення, слід зауважити, що саме такі центри є тим стримувальним чинником, який дає можливість, з одного боку, вказувати державним органам на їхні помилки та прорахунки і тим самим контролювати їх діяльність від імені незалежного громадянського суспільства; з іншого боку, за умов співпраці з чинною владою такі центри не менш ефективні, ніж державні, й спроможні допомогти владі в процесі ухвалення низки важливих стратегічних рішень. Головною їхньою перевагою є необтяженість державними бюрократичними процедурами. Найважливіше – зберігати незалежний статус та об'єктивність, що значною мірою залежить від джерел фінансування. Якщо експертні висновки, які виходять від недержавних центрів, будуть отримані внаслідок зовнішнього фінансування з боку різноманітних міжнародних представництв іноземних держав, а не з боку вітчизняного громадянського суспільства, то офіційна влада завжди сприйматиме їх з певною недовірою.

Логіку влади в цьому сенсі зрозуміти можна. Непоодинокими є приклади, коли представники українських економіко-політичних груп часто й самі не проти профінансувати різноманітні "псевдогромадські організації", діяльність яких спрямована не стільки на інтереси громадянського суспільства, скільки на обслуговування інтересів "основного донора". Я вже не кажу про різноманітну, пов'язану з таким станом речей конспірологію та навіяні минулим дискурси переслідування, зовнішньої загрози, існування внутрішнього та зовнішнього ворога тощо. До честі вітчизняного політичного істеблішменту, йому не властиві подібні манії.

У напрямі пошуку незалежних джерел фінансування позитивний вигляд має досвід Центру Олександра Разумкова, який постійно диверсифікує джерела фінансування, залучаючи для цього як вітчизняні, так і невітчизняні фонди, а з не вітчизняних – як американські, так і різноманітні європейські фундації, що є одним із чинників особливої довіри до результатів досліджень згаданого Центру.

Прикро, що певні аналітичні продукти недержавних аналітичних центрів справді гідні того, щоб бути реальною основою в процесі ухвалення рішень, і саме їх намагаються скомпрометувати. Передусім тут маються на увазі результати соціологічних досліджень. Останнім часом на вітчизняну незалежну соціологію було вилито стільки бруду щодо її "продажності", що хочеться її захистити, не відкидаючи при цьому реальність існування "замовних" соціологічних досліджень.

Корисним є створення постійно діючих груп, до яких входили би експерти з боку як держави, так і недержавних аналітичних центрів, із тенденціями до постійного розширення географічного представництва організацій-донорів, щоб якомога більше унеможливити спекуляції на тему "ангажованості".

7.7. ПОБУДОВА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ ЯК ПИТАННЯ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ БЕЗПЕКИ

Власюк О. С. Доповідь на 21-й Міжнародній конференції CODATA-21 "Наукова інформація для суспільства: від сьогодення в майбутнє" (Київ, 5–8 жовтня 2008 р.). *Публікується вперше.*

Дискусійна теза про те, що Україна – це один із найбільш динамічних і перспективних ринків світу, починає підтверджуватися. За даними, отриманими аналітиками лондонського "Економіст інтеліджанс юніт" (*Economist Intelligence Unit*), найбільш перспективними для ведення бізнесу на найближчі три-п'ять років за порядком рейтингів є 10 країн Східної та Південно-Східної Європи, у переліку яких Україна посідає почесну четверту позицію після Росії, Туреччини й Румунії.

На такі "молоді ринки" у минулому році припадала майже половина (49 %) світового споживання нафти. Вони споживали більше половини світового експорту з країн із розвиненою економікою, включно з інформаційними продуктами. На цих ринках було зосереджено до 70 % світових запасів конвертованої валюти (*forex*).

Успішна робота на українському та подібних до нього інформаційних ринках – головний ресурс, який намагаються із користю для себе використовувати транснаціональні *IT*-компанії. Найбільша проблема, пов'язана з використанням цього ресурсу, формулюється такими ТНК, як "розуміння місцевих споживачів". Під цим вони мають на увазі використання інтелектуального ресурсу схильних і здатних до інженерної творчості студентів. У 2007 р. бізнес офшорного програмування (аутсорсингу) дав в Україні прибуток у 246 млн дол. США, і в ньому було активно задіяно 7500 людей, переважно з-поміж тих самих студентів вищих технічних навчальних закладів, яких на той час налічувалося 670 тис. (за загального числа студентів 2,72 млн осіб).

Але Україні як державі важливо в цій ситуації дбати про власне майбутнє. Якісний рівень інформатизації України в добу глобального інформаційного суспільства має розглядатись як найважливіший показник захищеності національних інтересів. У цьому контексті доцільно привернути увагу громадськості та державних структур усіх рівнів, передусім тих, які відповідають за процеси інформатизації, на те, що Україна нині живе в умовах "дедлайнів" – жорстких термінів, відведених їй європейським і світовим співтовариством для впровадження низки стандартів сучасного інформаційного суспільства, зокрема тих, які стосуються різних елементів електронного врядування.

Сьогодні динамічно актуалізується проблема впровадження інформаційних технологій для ефективного забезпечення електронного урядування у найрізноманітніших сферах національної безпеки громадян, суспільства та держави.

Йдеться, зокрема, про проблему впровадження в Україні електронних паспортів (*e-passport*) із ключами електронного цифрового підпису та біометричною інформацією. Такі паспорти винятково важливі з погляду як упровадження ефективного електронного врядування, так і забезпечення ефективної боротьби з організованою злочинністю й тероризмом. На цьому тлі розмови

про порушення прав людини мають не зовсім доречний вигляд, оскільки найважливішим є право людини на життя.

Про впровадження електронних паспортів уже заявили понад 40 держав, серед яких Японія й більшість країн Євросоюзу. Зокрема, у Німеччині до червня 2009 р. будуть обов'язковими електронні паспорти другого покоління, в яких міститиметься інформація про відбитки пальців. Станом на січень 2008 р. електронні паспорти вже одержали більше 140 тис. росіян, а повністю на їх видачу Росія перейде до 2010 р.

У найближчій перспективі електронний паспорт стане обов'язковим і в Україні, оскільки наша держава як член Міжнародної організації цивільної авіації (*ICAO*) взяла на себе зобов'язання надати такі паспорти своїм громадянам до 1 квітня 2010 р.

В Україні діє план розвитку інформаційного суспільства, розрахований на 2007–2015 рр. Проте цей план не враховує того факту, що формування інформаційного суспільства та входження України до єдиного світового і європейського інформаційного простору пов'язані з різноманітними ризиками, викликами й загрозами. І тут не повинна вводити в оману загалом позитивна динаміка України в різноманітних міжнародних рейтингах "електронної готовності", за якими вона навіть випереджає Росію та інші країни СНД.

Якщо акцентувати увагу на тих елементах інформаційного суспільства, які пов'язані з електронною демократією, використанням Інтернет-технологій, можливостями мобільного зв'язку та цифрового телерадіомовлення для забезпечення інформаційної взаємодії органів влади з інститутами громадянського суспільства й бізнесу, то справи в нашій країні важко визнати задовільними.

Досить тривожним є те, що молода інформаційна індустрія України, по суті, ігнорує внутрішній, потенційно дуже потужний ринок, не робить ставки на розроблення власних програмних продуктів, які стосуються, зокрема, засобів системного програмного забезпечення інформаційної безпеки у найрізноманітніших сферах діяльності. Натомість домінує вже зазначена орієнтація на аутсорсинг, офшорне програмування тощо. Але на цих світових ринках конкуренція настільки висока, що представникам України, Росії та інших країн СНД "пробитися" важко. У кращому разі можна говорити про розробку програм на платформах західних виробників (*SAP, Oracle* тощо). Також зауважимо, що на ринках офшорного програмування домінують представники двох найпотужніших країн Азії – Індії та Китаю.

Тривожним є і той факт, що в Україні дотепер немає національних технічних парків, що ефективно діють, де вітчизняні фахівці могли б за пільгових податкових умов створювати вітчизняне програмне забезпечення для реалізації стратегічних інтересів власної держави. Можливо, саме тому більшість із цих фахівців нині змушені або працювати у себе вдома на закордонні компанії (аутсорсинг), або виїжджати за кордон.

Не вирішено питання використання в системі державного управління програмного забезпечення з відкритим кодом, що є загальноєвропейським трендом. Відповідні державні програми не фінансуються, а в системі державної служби переважає комерційне програмне забезпечення, яке до того ж далеко не завжди є ліцензійним.

Варто також звернути увагу на не вирішену досі проблему залучення наукового співтовариства до створення й реалізації програми ефективного захисту національного інформаційного простору, передбаченої проектом "Доктрини національної інформаційної безпеки", який невдовзі буде винесено на загальнонаціональне обговорення.

Зазначене є наслідком не лише того, що в Україні не сформувалося зріле громадянське суспільство, у якому найактивнішу експертну роль відігравало би наукове співтовариство, а й того, що наукові та освітні комунікації досі не здійснюються з використанням новітніх можливостей зв'язку, про що час від часу зауважує навіть Вища атестаційна комісія України.

Побудова інформаційного суспільства актуалізує також питання захисту інформаційного суверенітету – особливо в мережі Інтернет – з метою виховання в суспільстві належного рівня науково-раціональної культури та захисту від агресивної пропаганди псевдонауки, паранауки, різноманітного, замаскованого під науку, шахрайства тощо.

Принагідно варто згадати про істотне відставання у темпах розвитку українського сегмента Інтернету (Укрнету) від російського (Рунету): як кількісне, так і якісне, тобто як за приростом кількості відвідувачів мережі, так і за наповненням (контентом) Укрнету. Зокрема, фахівцями помічено, що з українського сегмента до російського сегмента Інтернету звертається у пошуках потрібної інформації вдесятеро більше відвідувачів, аніж навпаки.

До того ж порівняно з російськомовним сегментом вітчизняний сегмент мережі слабко використовується у наукових та освітніх комунікаціях. Варто звернути увагу й на той факт, що більшість вітчизняних Інтернет-ресурсів є російсько- або англомовними, що посилює небезпечну тенденцію до витіснення української мови не лише зі світової мережі, а й з наукового вжитку.

Нещодавно президент Росії Д. Медведєв особисто звернувся до корпорації *ICANN,* яка регулює доменні імена в Інтернеті, з пропозицією запровадити для реєстрації доменів та адрес у мережі кирилицю. На думку російського керівництва, це полегшить доступ до світової мережі для громадян, які погано володіють іноземними мовами, зокрема англійською.

У цьому конкретному випадку йдеться про серйозний виклик для України, оскільки російська ініціатива може призвести до відпливу частини вже створених україномовних сайтів (особливо тих, що належать комерційним компаніям і науковому співтовариству) до російського та російськомовного сегмента мережі.

Серед причин такого кількісного і якісного відставання у розвитку української мережі передусім слід назвати:

– слабкість вітчизняної телекомунікаційної інфраструктури, особливо на регіональному рівні;

– надто високі, як для пересічного українця, вартість комп'ютерів і тарифи на Інтернет-послуги;

– обмеженість інформаційних ресурсів у тій частині, що стосується безпосередньо України.

Якщо до цього додати відсутність надійних українізованих Інтернет-пошукачів та брак висококваліфікованих кадрів, то перспективи національного сегмента мережі не можна вважати обнадійливими.

Отже, Українська держава й наукове співтовариство безпосередньо мають заохочувати тих, хто активно використовує в мережі державну мову та пропагує національну культуру, включно з культурою науковою, підтримуючи і примножуючи належний рівень відповідних інформаційних ресурсів. Лише рухаючись таким шляхом, ми зможемо забезпечити справжній суверенітет держави і суспільства в інформаційній сфері.

7.8. ПРОБЛЕМИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

Власюк О. С. Виступ на відкритті Експертного "круглого столу" "Інформаційний суверенітет та відкритість державної влади в Україні" (Київ, НІПМБ, 17 червня 2008 р.). *Публікується вперше.*

Державна інформаційна політика належить сьогодні до пріоритетних напрямів розвитку української державності. Оскільки Українська держава не має реального суверенітету у власному інформаційному просторі, формується низка небезпек, викликів і загроз суспільному розвитку. Багато іноземних телекомпаній, радіостанцій, друкованих ЗМІ та Інтернет-видань відверто використовуються в інформаційно-психологічних операціях, які явно провадяться проти українських національних інтересів.

Симптоматично, що вісім авторитетних громадських організацій – "Просвіта", Конгрес української інтелігенції, Національна спілка письменників України, Українська всесвітня координаційна рада та ін. звернулися до української влади із заявою, в якій сказано, що "українська інформаційна політика є занадто ліберальною". Зазначені організації вимагали вжити відповідних заходів і, зокрема, "посилити особисту відповідальність редакторів і журналістів за озвучування антиукраїнських виступів російських політиків та експертів".

Далеко не всі керівники медіа і громадські та політичні діячі сприйняли такі дії як належну турботу про національні інтереси в інформаційній сфері. Частина медіа розцінила, зокрема, рішення РНБО України "Про невідкладні заходи щодо забезпечення інформаційної безпеки України" від 21 березня 2008 р. як замах на свободу слова. Інша частина намагалася зобразити справу так, ніби йдеться не про інформаційну безпеку держави й нації, а про контроль над інформаційними ресурсами. Керівництво деяких закордонних телерадіокомпаній обурилося тим, що РНБО України рекомендувала їм висвітлювати позиції офіційних осіб України, політичних партій, виконувати рішення Національної ради України з питань телебачення та радіомовлення і судових органів. Не отримала належного розуміння й вимога до закордонного телепродукту бути адаптованим до українських умов, особливо у мовному аспекті.

Не менш різкою є критика з боку "ліберальних кіл" позиції української влади щодо повернення народові України історичної пам'яті. Значна частина українських та російських медіа подає цю політику як формування і нав'язування нових історичних міфів, як репрезентацію української історії в дусі нескінченної боротьби з Росією тощо.

Отже, інформаційний суверенітет та відкритість державної влади є справді актуальною проблематикою, оскільки лише відкрита, але водночас суверенна інформаційна політика може бути істинною передумовою належного інформаційного забезпечення демократичного розвитку суспільства і держави. Тільки здійснюючи таку інформаційну політику, Україна посідатиме гідні й шановані позиції на світовій арені як впливова держава. Саме така інформаційна політика потрібна громадянам України, оскільки вона забезпечить реальну свободу слова й реальний громадянський контроль за діями та намірами влади, ефективні комунікації з центральною і місцевою владою.

На практиці зазначені імперативи суверенності та відкритості означають, що влада у всіх своїх діях і намірах зобов'язана рахуватися з нормативною базою, яка регулює процедури інформування громадян, механізми їх залучення до формування державної політики та оцінки якості влади. Але представники мас-медіа, включно із закордонними медіа, мають також рахуватися із зазначеними нормами та процедурами і не сприймати свободу як вседозволеність.

Варте уваги започаткування суспільних дискусій щодо пробудження національної пам'яті та примирення народу з власною, давньою й недавньою, історією. Тут є низка дискусійних проблем, пов'язаних із формуванням національної ідентичності держави і суспільства, як ключових завдань забезпечення національної безпеки України в інформаційній сфері.

У цьому контексті доцільно окреслити основні напрями української державної політики, спрямованої на утвердження національної пам'яті в умовах інформаційних війн, взаємозв'язок внутрішніх і зовнішніх вимірів утвердження національної ідентичності та реального інформаційного суверенітету. Важливо також розглянути питання формування національної ідентичності у контексті розвитку конкурентоспроможного й захищеного національного інформаційного простору. Йдеться про пошуки розумного балансу між відкритістю та закритістю, необхідного для захисту національних інтересів і забезпечення справжньої свободи слова й свободи діяльності засобів масової інформації та комунікації.

Слід зауважити, що питання забезпечення плідних відносин влади з масмедіа вже неодноразово обговорювалося на експертних зібраннях у трикутнику "представники влади – представники масмедіа – науковці та експерти". Інформаційна тематика сьогодні актуалізувалася не лише у стратегічному, а й у тактичному аспекті, оскільки відбувається серйозне загострення внутрішньополітичної боротьби. Тому особливо цінними є рецепти використання світового досвіду убезпечення боротьби політиків від зайвих крайнощів та переходу цієї боротьби у неприпустиму фазу, коли її заручником стають загальнонаціональні інтереси, а сама ця боротьба надмірно висвітлюється у масмедіа, набуває тенденцій до інтернаціоналізації. Світовий досвід відвернення таких загроз з великими труднощами імплементується в Україні.

Насамкінець варто наголосити, що інформаційний суверенітет та інформаційна відкритість – це значною мірою питання не лише політико-правові, а й питання етики та психології політичної діяльності, цивілізованого регулювання відносин політиків і державних службовців із масмедіа та журналістами.

Суверенність і відкритість української інформаційної політики – це також питання ефективного функціонування в Україні тих соціально-політичних інституцій, які є звичними для розвинених західних країн, але ще тільки розбудовуються в Україні, і які справді спроможні спрямувати дії влади на захист загальнонаціональних інтересів.

7.9. ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ

Власюк О. С. Виступ на "круглому столі" "Електронне врядування в системі національної безпеки держави" (Київ, НІПМБ, 18 листопада 2008 р.). *Публікується вперше.*

Одна з центральних проблем сьогодення – глобальна криза державного управління, конкретними проявами якої є криза парламентської демократії, зменшення ефективності демократичних інститутів, посилення політичного абсентеїзму, політичної фрустрації тощо. Причому це стосується не лише України як порівняно незрілої держави, а й більшості зрілих держав із різноманітними політичним режимами й формами устрою, починаючи від Російської Федерації та Китаю й закінчуючи США та країнами ЄС.

Зазначена криза керованості не в останню чергу пов'язана зі стрімким розвитком інформаційного суспільства, яке здійснює вирішальний вплив на комунікативні відносини між громадянами і державою, бізнесом і державою та відносини між державами й міждержавними та наддержавним угрупованнями.

Гострі дискусії викликає ключове питання щодо впливу мережі Інтернет на безпеку громадянина, суспільства і держави, на демократичні державні інституції і процеси державного та недержавного управління.

Незважаючи на розбіжності в оцінках наявних тенденцій, більшість аналітиків та експертів сходяться на тому, що розвиток Інтернету дав можливість досягти:

– результативнішого та ефективнішого державного управління;

– підвищення прозорості органів державної влади для громадян;

– ефективнішого зв'язку між політикою та політичним інституціями і громадянами та громадянським суспільством;

– активнішого залучення громадян до публічної політики та демократичних виборних процедур;

– практично значущого впливу громадян на підготовку, ухвалення та впровадження рішень на рівні як держави, так і структур громадянського суспільства.

Концепція побудови та функціонування демократичних інститутів у результаті широкого впровадження інформаційних технологій, яка отримала назву "електронної демократії", з'явилася на початку 1990-х років, коли настало розуміння того, що в глобальній комп'ютерній мережі закладено величезний потенціал революційних змін у процесах ухвалення державних рішень, створення й нарощування соціального капіталу, необхідного для зміцнення демократичних цінностей.

Поняття "електронний уряд" (*e-Government*), яке також з'явилося на початку 1990-х років, означає використання інформаційних і комунікативних технологій для підвищення ефективності діяльності уряду та можливого контролю над ним з боку громадянського суспільства. Йдеться передусім про свободу доступу до державної інформації, зміцнення довіри громадян до держави й політики, яку вона проводить як усередині країни, так і на міжнародній арені, про забезпечення необхідного рівня суспільного контролю за діяльністю державних органів та організацій, що сприяє покращенню міжнародного іміджу держави та довірі з боку іноземних інвесторів і міжнародних безпекових організацій.

В Україні, де електронне урядування робить лише перші кроки, вже в найближчій перспективі можна очікувати від нього нової якості надання послуг в електронному вигляді державними службами як громадянам, так і комерційним та бізнес-структурам (для отримання офіційних документів на різні дозволи, сплати податків і соціальних платежів, надання статистичної інформації тощо).

Тут, спираючись на позитивний досвід, набутий на шляху електронізації державного управління іншими країнами світу, можна розраховувати на:

– підвищення якості послуг для населення;

– орієнтацію на споживача;

– збільшення прозорості уряду для громадян та замовників;

– удосконалення інформаційних каналів взаємодії між урядом, бізнесом і громадянами;

– скорочення адміністративних витрат;

– зниження рівня різноманітних "спокус", які створюють приводи для корупції.

Із суто безпекової точки зору найважливішим здобутком електронного уряду є зростання рівня довіри суспільства до держави, подолання відчуження між ними, оскільки:

– реалізуються права кожного на вільне отримання інформації із загальнодоступних інформаційних ресурсів та інформаційних систем органів державної влади й управління;

– впроваджуються системи ідентифікації та підтвердження достовірності електронних документів, які циркулюють у комунікаційних системах.

Відповідно, з погляду національної безпеки ключовим для впровадження проекту *"e-Government"* в Україні є питання забезпечення прийнятного балансу принципів інформаційної відкритості та конфіденційності інформаційних потоків.

У зв'язку із зазначеним на сучасному етапі реалізації проекту *"e-Government"* потрібна чітка концепція забезпечення інформаційної безпеки, спроможна гарантувати контроль за використанням та захистом державних інформаційних систем і ресурсів від зловживань з боку державних службовців та користувачів. Такий захист можна забезпечити лише шляхом створення комплексної системи моніторингу та обліку операцій під час роботи з державними інформаційними системами, ресурсами й технологіями.

Водночас варто ще раз акцентувати увагу на тому, що створення "електронного уряду" є конструктивним заходом у напрямі подолання тенденції до

позиціонування України у світі як корумпованої держави з високим рівнем непрозорості та управлінської "тіні".

Насамкінець хотілося б підкреслити, що технології є лише засобом прогнозування та рушієм нових важливих тенденцій суспільного розвитку тією мірою, якою саме суспільство дозріло до цих технологій і готове керуватися новими ідеями, концептуальними конструкціями, що містять істотні соціальні інновації. Будь-яка технологія – навіть найпередовіша – є не творцем соціальних чи політичних змін і їх самоціллю, а лише засобом пришвидшення таких змін. Вона спрацьовує на краще лише за умови, що громадськість безпосередньо зацікавлена у вирішенні різноманітних громадських, безпекових та політичних питань, які впливають на щоденне життя цієї громадськості, що вона справді бажає бути вислуханою та почутою, а іноді навіть більшого – долучитися до активного політичного процесу з використанням новітніх інструментів "електронної демократії".

7.10. ДЕМОКРАТІЯ І МЕДІАКРАТІЯ: ПРОБЛЕМИ МЕДІА-ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ВІДКРИТОСТІ ТА ПРОЗОРОСТІ ДЕРЖАВНОЇ ВЛАДИ В УКРАЇНІ В УМОВАХ ДЕМОКРАТИЧНИХ ПЕРЕТВОРЕНЬ

Власюк О. С. Виступ на "круглому столі" "Світло та тіні соціально-економічного сьогодення України" (Київ, Ін-т політ. і етнонац. досліджень ім. І. Ф. Кураса НАН України, 19 червня 2008 р.). *Публікується вперше.*

За умов сучасної інформаційної революції державне управління неможливе без масмедіа, що повною мірою усвідомили українські політики. Щоправда, відносини медіа з українською владою і сферою політичних комунікацій складаються далеко не безконфліктно і є не завжди прозорими.

Разом з тим Україна, на відміну від багатьох інших країн пострадянського інформаційного простору, справедливо пишається здобутками у сфері свободи слова. В Україні справді немає безпосереднього адміністративно-державного втручання у діяльність каналів масмедіа, грубого маніпулювання громадської думкою, що є безумовним здобутком Помаранчевої революції 2004 р.

Водночас, з одного боку, українські політики проявляють до медіа (особливо до телебачення) настільки підвищену увагу, що часто підмінюють "телезірок", а популярні ток-шоу на провідних телеканалах мають вигляд прямого продовження засідань Верховної Ради, а з іншого – власники й менеджери потужних медіа-компаній (медійного "мейнстриму") активно втручаються у велику політику, не маючи на те жодного мандата народної довіри.

Якщо до цього додати відсутність в Україні засобів суспільного (публічного) телерадіомовлення, то картина зі станом свободи слова виявиться вкрай заплутаною й далеко не оптимістичною.

Вільні медіа і демократія в Україні виступають не як союзники, а як суперники в боротьбі за вплив на громадян. Незважаючи на спільність коріння їх

існування, в умовах нерозвиненого громадянського суспільства їхні відносини можуть перерости у взаємне поборювання і закінчитися погано як для демократичних свобод, так і для вільних медіа.

Медіакратія – це передусім наслідок реальної суперечності між ринком і демократією. Ринок, із медіа-ринком включно, має тенденцію до концентрації капіталів, унаслідок чого власниками переважної більшості медіа-ресурсів рано чи пізно стає невелика група "ринково зорієнтованих" підприємців. На противагу медіакратії, демократія – це справа загалу, тобто всього суспільства.

За умов розвиненої демократії інститут громадської думки, що формується під безпосереднім впливом мас-медіа, має всі можливості контролювати здійснення владних повноважень та легітимувати або, навпаки, делегітимувати дії влади як такі, що не відповідають суспільним очікуванням, які репрезентують медіа.

За умов нерозвиненої демократії та інститутів громадянського суспільства виникає об'єктивна загроза підміни народовладдя "медіавладдям", коли медіа, замість проміжної функції комунікатора між владою і громадянами, починають самостійно реалізувати владні функції.

Такі можливості викликали захоплення українських політиків нової хвилі, які вважають за потрібне постійно виступати у ролі продюсерів та акторів медіа-дійств. Як наслідок, на поверхні формується імітаційна модель влади та політичної участі (у вигляді натискання на кнопки представників нібито репрезентативної аудиторії в студії). Насправді це лише ілюзія політичної участі, під прикриттям якої здійснюється реальна "тіньова" влада.

Щоправда, переходи демократії та свободи слова у пряму протилежність – медіакратію (телекратію) – це не лише "дитяча хвороба" незрілих демократій, а й хвороба, що може уражати й більш зрілі демократичні організми, та не є принципово новою для розвинених демократичних суспільств. Тим більше – за умов інформаційної революції, коли екранна дійсність підмінила для багатьох людей первинні безпосередні відчуття.

Медіакратія – синдром, описаний французьким політиком та політологом Р. Дебре, близьким сподвижником легендарного Е. Гевари, а згодом радником колишнього президента Ф. Міттерана. Першопричиною медіакратії, як зазначали провідні західні дослідники, є надмірна некритична довіра певних верств населення до медіа-інформації. Жертвою такої довірливості стають зазвичай люди неосвічені, неспроможні самостійно збирати, обробляти й перевіряти інформацію на предмет її достовірності. В англійській мові суть справи гарно передає гра слів *mediacracy* й *mediocracy* (влада посередності, пересічності). Тобто влада великих медіа – це влада посередностей, пересічностей, якими вміло маніпулюють, – популізм.

Соціологічні опитування в Україні щодо довіри української аудиторії до масмедіа й, зокрема, дослідження, проведене соціологами в "революційному" 2004 р. на замовлення Асоціації видавців періодичної преси, свідчать про те, що з усіх соціальних інститутів лише церква має у населення більшу довіру, ніж ЗМІ (відсоток довіри до інституту церкви коливається зазвичай близько 70 %). Українським ЗМІ аудиторія довіряє більше, російським, як правило, – на 10 % менше, іншим іноземним ЗМІ (передусім західним) – ще менше.

Популярне у США зондування реакції внутрішньої та зарубіжної аудиторії на медіа-випливи, *Pew survey*, також свідчить про послідовне зростання, починаючи з 2004 р., влади великих медіакорпорацій над мисленням простих американців, а отже, над їхнім політичним вибором. Особливо піддатливими до впливів масмедіа є представники молодіжної аудиторії, третина яких вірить, за даними *Pew Research Center*, майже всім повідомленням медіа[1].

Серед політично заангажованих людей підвищеною навіюваністю характеризується аудиторія Демократичної партії, 45 % якої вірить "майже всьому", що виходить від *CNN*.

На додаток до медіа-навіювання перетворилася в нинішній Україні вулична мітингова "демократія", яка в тісному поєднанні з недоброчесними маніпулятивними медіа-впливами породжує різні спотворені версії культури "публічності", що межують з медіа-тероризмом і не мають нічого спільного з культурними та національно-історичними традиціями українського народу, з принципами справжнього народовладдя.

Спосіб вирішення будь-яких проблем, починаючи від побутових і закінчуючи політичними, на шляху "мітингування", доповненого видовищними картинками у вечірніх випусках теленовин, навіть породив у вітчизняному суспільстві особливу професію фахівця з "флешмобу", де є свої авторитети й законодавці моди (Д. Корчинський, В. Гладчук та ін.).

Неможливо заперечити право людей публічно обстоювати свої інтереси, виходячи для цього на майдани та вулиці, влаштовувати епатажні акції протесту, які привертають увагу медіа. Але одна справа, коли люди обстоюють конкретний індивідуальний, груповий або національний інтерес, і зовсім інша – коли протест провокують та роздмухують штучно, а одних і тих самих "протестантів" лідери різних політичних таборів виводять на вулиці з протилежними, але добре проплаченими вимогами. Ні до чого іншого, крім розхитування державності й інститутів демократії, це не призводить.

Тим часом відчуття нездоланності та вседозволеності "медіа-революційних акцій" перетворилося в нинішній Україні на серйозний чинник дискредитації всіх без винятку владних структур. Тим паче, що до небезпечної медійної гри долучилися представники всіх гілок влади та партійно-політичних таборів.

Фактично сьогодні "великі" українські масмедіа, контрольовані фінансово-олігархічними групами, мають ексклюзивні права на формування громадської думки щодо центральних проблем країни і варіантів їх вирішення, внаслідок чого влада чи політичні партії змушені перекладати мовою телевізійних медіа будь-яке рішення, щоб зацікавити споживача масової інформації у його впровадженні.

Потреба в зацікавленні (інтригуванні) споживача інформації зумовлює, у свою чергу, заміну істинного стану речей їх перцептивними образами, які мають "один до одного" відповідати потребам і очікуванням масової аудиторії.

Саме внаслідок такого медійного популізму постає небезпека переродження демократії в медіакратію, коли медіа перестають бути "сторожовими псами"

[1] *Key* News Audiences Now Blend Online and Traditional Sources Survey Reports // The Pew Research Center for the People & the Press. – 2008. – 17 Aug. [Електронний ресурс]. – Режим доступу : http://www.people-press.org/2008/08/17/key-news-audiences-now-blend-online-and-traditional-sources/

й ефективним знаряддям демократичних перетворень і починають спотворювати важливу для суспільства інформацію та поширювати дезорієнтуючі впливи. На практиці така трансформація призводить до театралізовано-розважального характеру всіх політичних заходів у їх екранних версіях, що робить їх схожими на "мильні опери".

Станом на весну 2009 р. маємо можливість щопонеділка (на каналі *ICTV*) і щоп'ятниці (на каналах "Інтер" та "Україна") спостерігати за "мильними сюжетами" з українського політичного життя. Постановники цих телевізійних дійств, починаючи з популярного С. Шустера й закінчуючи менш популярним А. Куликовим, беруть за основу телесюжетів конфлікти та міжособистісні протистояння справді "драматичні" і "непримиренні" (на зразок виборів спікера Верховної Ради України, формування коаліції, газових протистоянь з Росією тощо), але препарують усі ці справжні конфлікти до такого рівня зниження драматизму, коли громадяни-телеглядачі починають підозрювати, що вся ця екранна непримиренність – лише телевізійна гра, яка не має нічого спільного з реальним життям.

Наступним виявом виродження демократії у медіакратію є висловлювання політиками в радіо- та телеефірі "поставлених" думок і почуттів мовою медіа-штампів. При цьому в їхньому медіа-арсеналі з'являється забагато "правильних" слів (про демократію і свободу, права людини та захист вітчизняного виробника, верховенство права тощо), які жодним чином не кореспондують з поведінкою політичної сили, до якої вони належать, та й з їхньою власною політичною поведінкою.

Ще одним симптомом світової й української медіакратії є перетворення популярних публічних фігур на фігури великої політики (на зразок американця А. Шварценеггера, росіянина Й. Кобзона чи українських зірок шоу-бізнесу, великого спорту й телеекрана).

Підпорядковуючись жанрам і стилям масмедіа, сучасна українська політика дедалі більше деідеологізується та трансформується в елемент масової культури з її поверховою розважальністю. Це об'єктивно зумовлює загрозу перетворення медіа на засіб "промивання мізків" і переродження демократії за допомогою тих самих медіа на "керовану". Ідеться про деформації політичних комунікацій у трикутнику "влада – громадськість – медіа", коли офіційна влада неспроможна оперативно, коректно й переконливо реагувати на деструктивну поведінку масмедіа, не вдаючись до репресій і не наражаючись на звинувачення в обмеженні "свободи слова".

Отже, можна зробити такий висновок: в Україні є об'єктивна потреба у формуванні громадського інституту контролю за діяльністю масмедіа. Він повинен мати реальні можливості через масмедіа делегітимувати ті владні дії, що не відповідають суспільним очікуванням. Іншою, не менш важливою функцією такого інституту має стати протидія виродженню демократії в медіакратію. Очевидно, вагоме слово має сказати Національна комісія з утвердження свободи слова та розвитку інформаційної галузі при Президентові України.

Слід також ініціювати роботу постійно діючого Форуму громадських наглядових рад при провідних теле- і радіоканалах та інших впливових масмедіа. Першочерговим питанням для обговорення на такому Форумі може стати

прозорість власності на засоби масової інформації, оскільки сьогодні не лише громадськість, а й контролюючі державні органи не повною мірою поінформовані, кому належить певний засіб масової інформації та хто може впливати на його діяльність. Це потрібно для того, щоб поширювана ЗМІ інформація сприймалася громадськістю адекватно.

7.11. ЕЛЕКТРОННЕ УРЯДУВАННЯ ЯК ЧИННИК ПРОТИДІЇ КРИЗІ ДЕРЖАВНОГО УПРАВЛІННЯ

Власюк О. С. Матеріали до виступу на "Дні електронного урядування – 2009" (Київ, Нац. акад. держ. упр. при Президентові України, 14 травня 2009 р.). *Публікується вперше.*

Криза державного управління сьогодні набула глобального характеру. На підтвердження цього досить згадати нещодавні масові протести та заворушення у Франції, Греції, Німеччині, Литві, Ісландії, Туреччині, Молдові, Грузії тощо. До наведеного переліку можна додати практично всі держави – члени ООН, і легше перерахувати країни, де акцій протестів не було. Причини цих конфліктів різні, але в їх основі лежать глобальна причина – незадовільні комунікації між владою і суспільством. В Україні конкретними проявами цієї проблеми є криза парламентської демократії, низька ефективність демократичних інститутів, посилення в середовищі електорату настроїв політичного абсентеїзму тощо.

Отже, криза державного управління притаманна не лише країнам з порівняно незрілою демократією, а й більшості зрілих держав із різними політичним режимами та формами політичного устрою – від Російської Федерації й Китаю до США та країн ЄС.

Інформаційні технології з часом дедалі потужніше впливають на безпековий контекст комунікативних взаємодій між громадянами та державою, бізнесом і державою, між державами та міждержавними й наддержавним угрупованнями. Але технології не всесильні, а є лише провідником нових важливих тенденцій суспільного розвитку, причому тільки тією мірою, якою суспільство дозріло до цих технологій і готове керуватися новими ідеями та концептуальними конструкціями, що містять потенціал соціальних інновацій.

Будь-яка технологія – навіть найбільш передова – є не творцем соціальних чи політичних змін і самоціллю цих змін, а лише засобом пришвидшення таких змін. Отже, технологія спрацьовує тільки за умови, що суспільство безпосередньо зацікавлене у вирішенні різноманітних громадських, безпекових та політичних питань, які впливають на його щоденне життя. Це означає, що громадськість справді бажає бути вислуханою й почутою, а іноді навіть прагне долучитися до активного політичного процесу. Таку можливість сьогодні надають новітні інструменти електронної демократії.

Попит породжує пропозицію, і вже на початку 90-х років XX ст. з'явилися концепції електронної демократії та електронного уряду, що ґрунтуються на уявленнях про розбудову та функціонування демократичних інститутів на засадах упровадження інформаційних технологій. Згодом стало зрозумілим,

що в глобальній комп'ютерній мережі закладено величезний потенціал революційних змін у процесах ухвалення державних рішень, створення та нарощування соціального капіталу, необхідного для зміцнення демократичних цінностей.

Сказане стосується, зокрема, дискусій, які точаться нині в Україні щодо впливу мережі Інтернет на безпеку громадянина, суспільства і держави, на демократичні державні інституції та процеси державного й недержавного управління. Незважаючи на розбіжності в оцінках наявних тенденцій, більшість експертів сходяться на тому, що завдяки розвитку Інтернету було досягнуто:

– результативнішого та ефективнішого державного управління;

– підвищення прозорості органів державної влади для громадян;

– ефективнішого зв'язку між політикою та політичними інституціями і громадянами та громадянським суспільством;

– активнішого залучення громадян до публічної політики та демократичних виборних процедур;

– посилення впливу громадян на підготовку та впровадження рішень на рівні як держави, так і структур громадянського суспільства.

Поняття "електронний уряд" означає передусім використання інформаційно-комунікативних технологій для підвищення ефективності діяльності уряду і можливого контролю над ним з боку громадянського суспільства. Йдеться насамперед про свободу доступу до державної інформації, про зміцнення довіри громадян до держави й політики, яку вона проводить як усередині країни, так і на міжнародній арені, про забезпечення необхідного рівня суспільного контролю за діяльністю державних органів та організацій, що, зрештою, сприяє покращенню міжнародного іміджу держави та довірі до неї з боку іноземних інвесторів та міжнародних безпекових організацій.

В Україні, де електронне урядування сьогодні робить лише перші кроки, від нього вже в найближчій перспективі можна очікувати забезпечення нової якості надання державними службами в електронному вигляді найрізноманітніших послуг, як громадянам, так і бізнес-структурам: отримання офіційних документів на різні дозволи, сплата податків та соціальних платежів, надання статистичної інформації тощо.

Варто ще раз акцентувати на тому, що створення електронного уряду є конструктивним заходом у напрямі подолання тенденції до позиціонування України у світі як корумпованої держави з високим рівнем непрозорості та управлінської "тіні".

На шляху впровадження електронного урядування в Україні лежать дві ключові організаційно-методологічні проблеми.

1. З погляду методології національної безпеки, ключовим для впровадження проекту електронного урядування в Україні є питання забезпечення прийнятного балансу принципів інформаційної відкритості та конфіденційності інформаційних потоків. У зв'язку з цим на нинішньому етапі реалізації цього проекту потрібна чітка концепція забезпечення інформаційної безпеки, спроможна забезпечити контроль за використанням та захистом державних інформаційних систем і ресурсів від зловживань з боку як державних службовців, так і користувачів. Такий захист можна забезпечити лише за допомогою створення

комплексної системи моніторингу та обліку операцій під час роботи з державними інформаційними системами, ресурсами й технологіями, а це нелегке завдання.

2. Зрозуміло, що для використання електронного інструменту демократії необхідне належне юридичне підґрунтя, яке легалізуватиме таку форму комунікації між громадськістю та державними установами. Труднощі юридичного характеру можуть виникати вже на етапі збирання підписів під петиціями й зверненнями.

Особливо це стосується України, де електронні підписи, а відповідно й процедура ідентифікації поки що не перетворилися на звичні атрибути суспільного життя, як у більшості країн світу з розвиненими формами та процедурами демократії. Для підтвердження справжності волевиявлення в Україні дотепер необхідні "традиційні" засоби верифікації шляхом безпосереднього контакту із заявниками, перевірки адресних даних за допомогою довідкових служб тощо. Водночас не укладено єдиного реєстру виборців. Отже, в Україні на шляху становлення електронної демократії належить вирішити проблему електронного підпису.

Цю проблему варто розглядати в більш широкому контексті – як досі не вирішену в Україні проблему впровадження електронних паспортів (*e-Passport*) з ключами електронного цифрового підпису та біометричною інформацією. Такі паспорти винятково важливі з погляду як упровадження ефективного електронного урядування, так і забезпечення ефективної боротьби з організованою злочинністю та тероризмом. На цьому тлі не зовсім доречний вигляд мають розмови про порушення прав людини, про закодоване в електронних паспортах "число диявола" тощо, адже найважливішим є право людини на життя.

7.12. ДО ПИТАННЯ ЕКСПЕРТНО-АНАЛІТИЧНОЇ ПІДТРИМКИ УХВАЛЕННЯ ДЕРЖАВНИХ РІШЕНЬ

Власюк О. С. Виступ на відкритті "круглого столу" "Інформаційна прозорість та експертна підтримка ухвалення державних рішень" (Київ, НІПМБ, 16 грудня 2009 р.). *Публікується вперше.*

У достовірності вислову "Хто володіє інформацією, той володіє світом" нині, в добу розвитку інформаційних технологій, певно, не сумнівається ніхто. Можна лише дещо уточнити цю формулу: не тільки володіє, а й уміє її аналізувати, обробляти, правильно інтерпретувати і робити на підставі цього виважені висновки. Більше того, за сучасних умов аналіз та експертна оцінка зібраної інформації є визначальними передумовами ухвалення ефективних політичних і економічних рішень.

Тобто проблема полягає не стільки в отриманні певної інформації, скільки в її аналізі, а саме у відокремленні від достовірної та релевантної інформації так званих шумів. Важлива також правильна інтерпретація інформації: її відповідність (релевантність) потребам майбутніх рішень влади для забезпечення національних інтересів. Вимоги до інформаційно-аналітичної роботи в структурі влади можна концентровано сформулювати у вигляді слогана: "Інформувати владу вчасно, точно, зрозуміло!".

Якість інформації, що циркулює в системі владних відносин та системі підготовки, ухвалення й імплементації рішень, залежить передусім від прозорості та транспарентності зазначених процесів. За так званого тіньового лобіювання, поширеного в Україні, маємо справді грубі викривлення фактів та підходів до їх тлумачення. Інформаційна картина реального світу спотворюється на догоду певним групам інтересів, які часто вельми далекі від інтересів національних. Отже, проблема є не тільки експертною, а й політичною.

У контексті цієї проблематики на увагу заслуговує система забезпечення збирання, аналітичного оброблення та експертного оцінювання інформації, що діє у США. У ній вирізняють такі три складники:

– державні інформаційні органи, розвідувальна спільнота, установи Державного департаменту, Адміністрації президента, Ради національної безпеки;

– інформаційні центри безпосередньої підтримки ухвалення рішень, до яких належать такі установи, як корпорація *RAND*, Військовий університет національної оборони тощо;

– громадські центри "широкої підтримки", зокрема такі як Рада із зовнішньої політики, Центр стратегічних і міжнародних досліджень, Американський підприємницький інститут, Фонд "Спадщина", Інститут Като, Атлантична рада, Центр національної політики.

Перший складник системи експертно-аналітичної підтримки ухвалення державних рішень забезпечує оперативне керівництво державою, інтереси групи безпосередньої підтримки зосереджені на стратегічному рівні, а третя група, яку можна назвати громадською, формує "політичний порядок денний", здійснює стратегічне планування зовнішньополітичної діяльності.

Ситуація, що нині склалася в Україні, з отриманням і обробленням "міжнародної інформації" та експертною підтримкою ухвалення державних рішень у сфері міжнародної і безпекової політики із суто формального погляду максимально наближена до американської чи європейської, але цілком зрозуміло, що з реалістичного погляду вона дуже далека від цивілізованого ідеалу.

В Україні діє Державний комітет телебачення та радіомовлення, відповідальний за здійснення інформаційної політики, який, щоправда, втратив не тільки попередню назву – Державний комітет інформаційної політики, а й чималу частку повноважень. Важливі інформаційно-аналітичні функції виконує структурний підрозділ цього комітету – Укрінформ.

У 1992 р. розпочав діяльність Національний інститут стратегічних досліджень, який за статутом є "урядовою інституцією для проведення досліджень, аналітичного прогнозування та стратегічного планування з метою забезпечення інформацією Ради національної безпеки і оборони та Президента України". Функціонують відповідні підрозділи Секретаріату Президента України, Секретаріату Кабінету Міністрів України та Апарату Ради національної безпеки і оборони України. У структурі РНБО України діють три науково-аналітичні центри, до яких належить і Національний інститут проблем міжнародної безпеки.

Відповідні інформаційно-аналітичні та експертні підрозділи працюють у структурі Міністерства закордонних справ України, Служби безпеки України, Міністерства оборони України, Державного комітету у справах охорони

державного кордону України. Діяльність українських спецслужб у сфері розвідки координує Комітет з питань розвідки при Президентові України. Поступово створюється також недержавне інформаційно-аналітичне середовище, передусім відповідні інститути Національної академії наук України. Формуються незалежні інформаційно-аналітичні центри.

Водночас слід відверто визнати, що інформаційно-аналітичне середовище в Україні ще далеке від вимог часу та потребує певної корекції у напрямі посилення незалежності науково-аналітичних інституцій від політичних впливів, формування професійної фахової спільноти тощо.

7.13. МОНІТОРИНГ ІНФОРМАЦІЇ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Власюк О. С. Виступ на відкритті "круглого столу" "Моніторинг та прогнозування у системі національної безпеки України" (Київ, НІПМБ, 25 червня 2009 р.). *Публікується вперше.*

Моніторинг – це спеціально організоване, систематичне спостереження за станом об'єктів, явищ, процесів з метою їх оцінки, контролю, прогнозування. Нагадаємо, що лат. *monito*, покладене в основу терміна "моніторинг", означає "попереджаю" і є співзвучним з іншим латинським словом *munito* – "озброюватися". Звідси класичний афоризм: "Попереджений – отже, озброєний!" (*Premonitus – premunitus!*).

Будь-яка серйозна аналітика починається з моніторингу, який є її обов'язковим підготовчим етапом. Без невпинного системного відстеження певного об'єкта, процесу, явища, ситуації тощо годі говорити про аналіз і висновки, придатні для ухвалення керівних та управлінських рішень. Зазвичай тут ідеться про управлінські консенсусні технології, пов'язані з необхідністю вибору найоптимальніших альтернатив серед усіх можливих та таких, що конкурують між собою, версій (принцип "найменшого зла"). Труднощі, пов'язані з цим, зумовлені тими основними чинниками, які не задіяні у прикінцевому ухваленні рішення, але мають істотне значення на етапах збирання та опрацювання вихідної інформації, її структурування і класифікації.

Проблема моніторингу та критеріальних системних оцінок в ухваленні оптимальних рішень має, на нашу думку, формулюватися під кутом зору подолання кризи керованості у різноманітних сферах державного та соціального життя сучасної України. Методологією такого підходу є один з оригінальних напрямів сучасного системного руху – концептуальне проектування систем організаційного управління.

Наразі подібний підхід не отримав належного розуміння та розвитку в Україні, що мало б, на наш погляд, бути предметом нинішнього експертного обговорення. Пропонуємо вашій увазі узагальнення нашого скромного досвіду проведення моніторингу.

Міжнародний моніторинг є інформаційно-аналітичним оглядом значущих міжнародних подій у контексті їх актуальності для міжнародного позиціювання України, зовнішньої і безпекової політики країни.

Інформаційно-аналітичні матеріали до моніторингу доцільно готувати у вигляді окремих "повідомлень", структурованих за сферами досліджень (міжнародні відносини, глобальна і регіональна безпека, міжнародна економіка, соціальна політика тощо) або за актуальною проблематикою (світова фінансово-економічна криза, боротьба з тероризмом тощо).

Структура повідомлення в моніторингу має містити чотири взаємопов'язані елементи: "подія – ситуація", "тенденція – прогноз", "виклики – загрози", "реагування – заходи". Елемент повідомлення "подія – ситуація" є викладом сутності події, яка містить реальні або потенційні виклики й загрози, що пов'язано зі стислим описом й оцінкою дій, заяв, рішень, нормативно-правових документів національних урядів (лідерів держав), міжнародних організацій або впливових транснаціональних структур, як і окремих впливових персоналій (духовних лідерів, наукових авторитетів, ватажків міжнародних кримінальних структур та ін.). Ідеться також про суттєві зміни у міжнародній ситуації в окремих регіонах і країнах, міждержавних відносинах тощо.

Головний критерій відбору "події" для моніторингу та аналітичного опрацювання – її актуальність у контексті міжнародного позиціювання, зовнішньої і безпекової політики України; реального (потенційного) зовнішньополітичного впливу на стан національної безпеки України. Звідси випливає доцільність урахування як самої події (ситуації), так і її наслідків у виробленні та впровадженні внутрішньої й зовнішньої політики України.

Обов'язковими атрибутами висвітлення події є час, місце, учасники, джерела інформації (особливо якщо виникають сумніви щодо об'єктивності висвітлення події).

Елемент повідомлення "тенденція – прогноз" передбачає виклад аналітичних припущень про причини і рушійні сили події, подальший розвиток ситуації (коротко-, середньо- та довготермінові тенденції), ймовірні наслідки для національної безпеки України.

Насамкінець слід нагадати, що аналітичні матеріали концептуального змісту з моніторингом включно, на відміну від дискурсів ідеологічного або публіцистичного ґатунку, мають бути витримані в дусі "політкоректності". На практиці це означає, що аналітика не повинна бути ідеологічно чи персонально ангажованою, не повинна надавати аргументи "за" або "проти" на догоду різним протиборчим політичним силам. Саме вищий рівень відрізняє аналітику від журналістики.

Проте викладене зовсім не означає, що моніторинг і аналітика перебувають поза цінностями та оцінками, відповідно до відомого ідеалу "позитивної науки". Їхня сутність полягає в іншому. Цінність предметного багатоаспектного аналізу в аналітиці бере гору над конфронтаційним ідеологічним "рефлексом".

Усе це, вочевидь, означає необхідність формування і в суспільстві загалом, і в державних та недержавних структурах дослідницької культури систематизації цінностей і оцінок згідно з певною усталеною шкалою суспільно значущих норм та нормативів, приведення застосовуваних аналітиком предметних оцінок до рівня критеріально прозорої, наперед визначеної, структури, надання цій структурі концептуального, нормативного характеру. Головне питання полягає в придатності структури системних моніторингових та аналітичних оцінок для потреб практики управління у сфері національної безпеки.

7.14. ТЕХНОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ВІЙНИ В УМОВАХ ЕКОНОМІЧНОЇ КРИЗИ ТА ПОЛІТИЧНОЇ НЕВИЗНАЧЕНОСТІ В УКРАЇНІ

Власюк О. С., Недбаєвський С. Л. Матеріали до аналітичної довідки (Київ, НІПМБ, червень 2009 р.). *Публікується вперше.*

Україна переживає складний період суспільного життя. В умовах поглиблення фінансово-економічної кризи, наростання політичної невизначеності, зумовленої переформатуванням політичної еліти та практично вже започаткованою президентською кампанією, в українському суспільстві стрімко посилюється соціально-політична нестабільність. Це створює спокусу для певних закордонних політичних кіл активно проштовхувати в Україні свої політичні, економічні та ідеологічні інтереси. Закономірно, що такі спроби супроводжуються масштабними інформаційними кампаніями, мають на меті легітимізувати в українській суспільній думці втручання в її суверенні справи тепер і в майбутньому.

Нинішнє протистояння в українському інформаційному просторі зазнало певних змін як у концептуальному (змістовому), так і в технологічному (у засобах оперування масовою інформацією та її поширення на території України) вимірах.

Концептуальні зміни інформаційної політики Росії на українському напрямі

Останнім часом в інформаційній політиці Росії щодо України означилися такі тенденції.

1. Порівняно з пропагандистськими кампаніями перших років президентства Віктора Ющенка, в яких були задіяні величезні інформаційні ресурси для боротьби з українським "помаранчевим проектом", нинішня ситуація в міждержавних інформаційних відносинах з першого погляду створює враження "пропагандистського затишшя".

2. Спостерігається певна відмова від риторики ескалації конфлікту та практики впровадження інформаційних конфліктних технологій, насамперед від мусування тези про цивілізаційний розкол України по лінії "Схід/Захід".

3. Пом'якшуються критичні коментарі щодо євроатлантичної інтеграції України.

4. Відбувається відхід від тактики нав'язливого "смакування" помилок "помаранчевої влади", тотальної дискредитації управлінського стилю та іміджу Президента України.

Усі ці та інші ознаки свідчать про відмову організаторів російської інформаційної політики від стратегії прямого інформаційного тиску в українському інформаційному просторі, відкритої боротьби проти "помаранчевого проекту" (що, як і раніше, сприймається Кремлем як пряма загроза безпеці Росії). З одного боку, така відмова пов'язана з усвідомленням певною частиною архітекторів російської інформаційної політики її неефективності на українському напрямі, внаслідок чого "Росія стала союзником Ющенка щодо відокремлення росіян

від українців"[2], з іншого – з кризовими явищами в українському політикумі та наближенням виборів: російська влада очікує змін у зовнішньополітичній стратегії України та, відповідно, у форматі українсько-російських відносин.

Замість стратегії відкритого інформаційного протистояння українській владі в Росії формується більш гнучка та небезпечна стратегія знецінення українського національно-державного проекту як такого. Підступність цієї стратегії полягає в тому, що при зменшенні загального обсягу конфронтаційної риторики на адресу України спричинений ефект (відчуття хаосу та дезорієнтації в українських споживачів інформації) є на порядок більшим. Такий ефект досягається за рахунок витончених акцентів на спеціально відібраних темах, здатних впливати на найбільш уразливі сфери масової свідомості.

1. Тема слабкості (або навіть відсутності) усвідомлення українцями національної ідентичності у формі натяків у контексті більш загальних квазітеоретичних міркувань про "неспроможні держави", а також мусування теми про неповний суверенітет української держави над своїми територіями.

2. "Розщеплення" українських реалій: повідомлення про Україну, як правило, містить констатацію двох (або більше) непримиренних позицій у владі та соціумі, а також відбувається "смакування" їх конфлікту.

3. Повідомлення про Україну здебільшого натякає на самодеструктивність української влади, а також, по можливості, демонструються безглузді та анекдотичні аспекти українського суспільно-політичного життя. Сама тема української незалежності трактується як самокатування – спроба "невід'ємної частини" відірватись від "цілого" (нерозривного "історичного тіла" спільної батьківщини).

4. Цілеспрямоване роздмухування внутрішнього соціального конфлікту: заздрощів щодо заможних співвітчизників (олігархів та можновладців) і протиставлення однієї соціальної страти іншим. Ця технологія є випробуваним часом методом провокування соціальної агресії та суспільного хаосу.

5. Підтримка катастрофічних настроїв та очікувань у будь-якій формі – від публікування "поганих гороскопів" для України до псевдонаукових експертних прогнозів близького дефолту.

Підступність технології знецінення полягає в її прихованому характері. Вона влучно маскується під громадську критику, націлену на викриття та подолання соціальних викривлень і недоліків. Головна відмінність технології знецінення від конструктивної громадської критики полягає в тому, що вона не спрямована на розвиток суспільства шляхом усунення його недоліків. Її мета – не орієнтувати і мобілізувати маси на позитивні зрушення, а творити розпач та хаос у головах людей і, як наслідок, поширювати масову зневіру та неприязнь до всього українського.

За формою знецінення найчастіше набуває вигляду бурчання (рос. – "брюзжание"). І хоча більшість людей сприймає бурчання вкрай негативно, якщо йдеться про феномени масової пропаганди, масштабне використання такої тональності може спричинити значний ефект – активізувати у підсвідомості злоякісні депресивні зони, здатні загнати людей у розпач.

---

[2] *Мороз С.* Россия как союзница Ющенко / С. Мороз [Електронний ресурс]. – Режим доступу : http://www.rosbalt.ru/2009/01/28/613376.html

Російські медіа висвітлюють перебіг глобальної економічної кризи в Україні так, що у споживача інформації не залишається сумнівів у неминучості краху української економіки і всього проекту української незалежності.

Найбільш резонансною інформаційною подією останнього часу з теми "неспроможності" Української держави стало інтерв'ю С. Караганова кореспондентові "Російського журналу"[3], в якому автор чітко, без зайвих дипломатичних евівоків висловлює позицію Кремля щодо української незалежності. Нинішній стан України голова президії Ради із зовнішньої та оборонної політики РФ оцінює як "скажену десуверенізацію" і "розпад держави", пророкуючи Україні в найближчі півтора року місце у зростаючій групі країн, що підпадають під визначення *failed state* ("неспроможна держава").

Однією з найбільш мусованих російською пропагандою тем залишається зовнішня керованість України. Зокрема, російський політолог, депутат Державної думи, С. Марков робить таку "констатацію": "Якщо розібратися, Україна сьогодні є суверенною не більш ніж на 40 %, тому що провідні інститути державності цієї країни виведені з-під контролю держави". Головні серед них, на думку депутата, – СБУ, Міністерство оборони і МЗС. Частково контролюються ззовні система освіти, ЗМІ та інші гуманітарні галузі[4].

Подібна установка щодо української незалежності формується на найвищому рівні російської влади. Так, нещодавно В. Путін під час покладання квітів до пам'ятника генералові А. Денікіну навів імперські міркування Денікіна про єдність "Великої і Малої Росії" і заявив, що "нікому не має бути дозволено втручатися у відносини між нами, це завжди було справою самої Росії!"[5]. До того ж і в Україні є чимало сил, що ретранслюють російський погляд на ситуацію.

Технічні новації та можливості їх використання в інформаційній війні

Недавні події в Молдові виявили нові тенденції до використання інформаційних технологій в організації дій, що дестабілізують соціально-політичну ситуацію в країні. Ці тенденції в основному вкладаються в рамки стратегії мережевого управління, головною ознакою якої на сучасному етапі є інтенсивне використання популярних соціальних мереж в Інтернеті, зокрема мережі *Twitter*, для маніпуляції свідомістю і поведінкою великих мас людей.

Twitter – не лише нова високотехнологічна система комунікації, здатна протягом короткого часу мобілізувати велику кількість людей. Це також система групоутворення і структуризації соціального простору – практична реалізація інформаційної концепції дворівневої комунікації. Відповідно до згаданої концепції, інформація, яка поширюється в мережі, не впливає безпосередньо на суспільство; її сприймають спершу окремі особи (неформальні

[3] *Караганов С.* Украина – это вообще непонятно что такое / С. Караганов [Електронний ресурс]. – Режим доступу : http://republic.com.ua/aboutus.php?id_show=9902

[4] *Торшина С.* Кто сыграет на трубе? / С. Торшина // Аргументы и факты в Украине. – 2009. – № 19 [Електронний ресурс]. – Режим доступу : http://www.ukr.aif.ru/society/article/17440

[5] *Путин* посоветовал журналистам читать дневники Деникина // УНІАН. – 2009. – 24 травня [Електронний ресурс]. – Режим доступу : http://unian.net/rus/news/news-317307.html.

лідери – модератори), що на базі цієї інформації створюють відповідні ідеї і настрої, які потім доносять до інших людей завдяки своїй лідерській харизмі.

Технологічним надбанням соціальних мереж, подібних до *Twitter*, є нова якість їх інтерактивності. Повідомлення можуть автоматично поширюватись у режимі електронної пошти, *SMS*-повідомлень, телефонного додзвону тощо. Мережа не тільки "розмовляє" з людиною в діалоговому режимі, а й сама "знаходить" її за допомогою мобільного телефону. Контакт стає дедалі більш особистісним, вимагає від абонента більше часу на перебування в мережі та "відповідальнішого" ставлення до можливості самовільного виходу з неї. Тобто з психологічного погляду спостерігається тенденція до поглиблення мережевої залежності та зростання керованості великої кількості Інтернет-користувачів.

Особливу увагу привертають можливості, що відкриваються при використанні нових Інтернет-технологій у передвиборчих кампаніях. У цьому контексті за зразок видається кампанія Б. Обами. У західних ЗМІ поширена думка, що саме Інтернет-піар зробив Б. Обаму президентом США. Справді, PR-менеджери "нової медіа-кампанії" Б. Обами використали весь спектр електронних засобів комунікації – від *YouTube* та електронної пошти до блогів і *Facebook*. Як наслідок, 13 млн американців передплатили розсилання повідомлень передвиборчого штабу електронною поштою, було зібрано пожертви на адресу передвиборчого штабу від 3,95 млн осіб, а також організовано віртуальний клуб шанувальників Б. Обами з 3,2 млн користувачів у *Facebook*. Через мережу було зібрано 500 млн дол. США, що становить 2/3 від загальної кількості пожертв на виборчу кампанію Б. Обами. За допомогою координації через Інтернет було проведено понад 200 тис. акцій на підтримку Б. Обами і створено близько 40 тис. груп добровільних агітаторів у різних містах США. Ці групи виявились настільки стійкими, що існують донині.

На відміну від традиційних медіа-кампаній, націлених на тих, хто ще не визначився з вибором, Інтернет-кампанія медіадиректора передвиборчого штабу Б. Обами Дж. Роспарса була спрямована на підтримку і дистанційне керування прихильниками Б. Обами на місцях. У кращих традиціях мережевого управління команда Дж. Роспарса лише визначала ключові теми та ідеї, а люди на місцях об'єднували зусилля в агітації за Б. Обаму, діючи самостійно, без вказівок згори. Відсутність необхідності виконувати "розпорядження згори" викликала в учасників подій відчуття особистої відповідальності за справу, що дуже імпонує людям. А можливість безпосереднього спілкування як між собою, так і через мережу з керівниками штабу створювала ефект психотерапевтичних "груп зустрічей", де кожен учасник отримує своєрідні психологічні дивіденди від відчуття особистої причетності до своєї групи, а також до загальної справи.

За деякими джерелами, російські політтехнологи нині активно опановують технологію мережевого управління, зокрема щодо українського інформаційного простору. Деякі молодіжні організації проросійського спрямування в Криму і на південному сході країни ("Антифа" та ін.) за структурою та характером активності нагадують мережевоцентровані. Відсутність чіткого лідера, жорсткої ієрархії ухвалення і виконання управлінських рішень, широке застосування "креативу знизу", а також інші ознаки свідчать про те, що діє саме мережевий принцип групоутворення і зовнішнього керування.

Російськозалежні політичні медіа в українському інформаційному просторі є добре налагодженою пропагандистською машиною, що структурована і працює за мережевим принципом: навіть якщо з будь-яких причин не надходить конкретна команда згори, всі вони "знають", яку інформацію і як необхідно подавати аудиторії. Таким чином, рівень присутності та технологічні можливості російських і російськозалежних ресурсів в українському інформаційному просторі достатні для проведення масштабних інформаційних операцій, спрямованих на вирішення конкретних політичних завдань російської влади на території України.

Щоб подолати цей стан речей, слід вжити такі заходи.

1. Одним із першочергових завдань для українських медіа на нинішньому етапі є деконструкція дискурсу знецінювання у всіх його проявах щодо української держави та спростування катастрофічних сценаріїв розвитку подій в Україні як найбільш небезпечних засобів маніпулювання громадською думкою.

2. Необхідно розгорнути масштабну інформаційну роботу з роз'яснення українській аудиторії того, що ідея широкої парламентської коаліції і плани щодо зменшення ролі інституту президентства перебувають у руслі російської стратегії знецінення української незалежності. Інститут президента є символом та гарантом українського суверенітету, і підрив його авторитету може призвести до непоправних стратегічних втрат.

3. Потрібні нові кроки щодо розширення патріотичного сегмента вітчизняного інформаційного простору за рахунок інвестицій в інформаційну сферу, а також упровадження екстрених заходів, спрямованих на звуження маневру лобістам іноземних політичних інтересів в українському інформаційному просторі.

4. Слід відстежувати прояви використання технології мережевого управління в Україні, зосередивши головну увагу на молодіжному сегменті українського соціуму. З метою протидії збільшенню кількості проросійських молодіжних організацій мережевого типу в Україні треба проводити активну і послідовну молодіжну політику, зокрема сприяти зростанню чисельності в країні молодіжних та інших громадських організацій патріотичної спрямованості.

7.15. ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРОВІДНИМИ ДЕРЖАВАМИ СВІТУ: ВИСНОВКИ ДЛЯ УКРАЇНИ

Власюк О. С., Ожеван М. А., Дубов Д. В. Матеріали до аналітичної довідки (Київ, НІПМБ, серпень 2009 р.). *Публікується вперше.*

З початку 2009 р. з боку провідних країн світу (США, Німеччина, Велика Британія) та міжнародних організацій (НАТО) значно зростає зацікавленість до проблеми посилення власної кібербезпеки та розробки наступальних засобів ведення кібервійн. Це зумовлено:

– збільшенням кількості кримінальних злочинів, що вчинюються в кіберпросторі (переважно шахрайства з пластиковими картками);

– посиленням проникнення інформаційних технологій у всі сфери суспільного життя, зокрема ті, що відповідають за життєдіяльність суспільства загалом (енергетика, житлово-комунальне господарство, фінанси тощо);

– посиленням уваги до наступальних можливостей кіберпростору з боку Китаю, Північної Кореї, деяких мусульманських країн.

Головний тренд у цьому процесі задає нова Адміністрація США, яка із самого початку діяльності актуалізувала проблему захисту національного кіберпростору та артикулювала бажання займати активнішу позицію щодо розвитку наступальних кібертехнологій.

Ще наприкінці квітня 2009 р. американські сенатори О. Сноу та Дж. Рокфеллер підготували законопроект[6], що надасть президенту США Б. Обамі доступ до "другої червоної кнопки", за допомогою якої він зможе у надзвичайних випадках загроз національній безпеці відключати доступ до мережі Інтернет на всій території США. Крім того, 9 липня 2009 р. сенатор К. Джилібренд запропонував законопроект[7], згідно з яким США зможуть співпрацювати з будь-яким урядом світу, для організації глобальної відсічі нападникам у кіберпросторі. Законопроект запрацює лише у разі підписання відповідних міжнародних угод, а поки що поширюватиметься лише на співпрацю США з найближчими союзниками, передусім Великою Британією. Крім того, з метою посилення контролю за мережею Інтернет, уряд США на 2010 р. виділив ФБР додатково 234 млн дол. США для спеціального проекту з прослуховування Інтернету *(Advanced Electronic Surveillance – Going Dark)*[8], насамперед спрямованого на забезпечення можливості прослуховування Інтернет-комунікаторів (наприклад, *Skype*).

29 травня 2009 р. на вимогу президента США Б. Обами підготовлений "Огляд кібербезпекової політики"[9], у якому виділено низку ключових тез, центральна серед яких: "Білий дім має стати лідером у питаннях координації, розроблення та впровадження новітніх стандартів кібербезпеки Америки". Для реалізації цієї ідеї підкреслювалася важливість здійснення організаційних заходів, що мають сформувати нову архітектуру системи національної кібербезпеки.

Вже 1 червня 2009 р. президент США оголосив про створення при Білому домі відділу з кібербезпеки, до обов'язків якого належатимуть координація роботи урядових відомств, що займаються комп'ютерною безпекою, розслідуванням кіберзлочинів та хакерських атак, а також розроблення нових захисних технологій. Керівник нового відділу звітуватиме перед Радою національної безпеки та Економічною радою, а також регулярно зустрічатиметься з президентом. Також планується створити в адміністрації дві нові посади з питань реалізації державної *IT*-стратегії (швидше за все, цивільна особа) та забезпечення безпеки федеральних і військових комп'ютерних мереж (військовий).

Повідомленню про створення нового відділу передували публікація в газеті *The New York Times* та офіційна заява Б. Обами. Так, 29 травня в *The New York Times* з'явилося повідомлення про бажання керівництва Пентагону створити

---

[6] *The Cybersecurity* Act of 2009 [Електронний ресурс]. – Режим доступу : http://www.snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=8D76A8BB-802A-23AD-4384-78D04C8509A9

[7] *Fostering* a Global Response to Cyber Attacks Act (Introduced in Senate) [Електронний ресурс]. – Режим доступу : http://thomas.loc.gov/cgi-bin/query/z?c111: S.1438

[8] *ФБР* получит $ 234 миллиона на новые средства слежки за Интернетом [Електронний ресурс]. – Режим доступу : http://hitech.newsru.com/article/15jun2009 /fbi

[9] *Cyberspace* Policy Review [Електронний ресурс]. – Режим доступу : http://www.whitehouse.gov/asset.aspx?AssetId=1732

спеціальне командування для ведення війн у кіберпросторі. 30 травня Б. Обама виступив із заявою, в якій охарактеризував усю цифрову інфраструктуру (мережі та комп'ютери) як "стратегічне національне надбання" і запевнив, що будь-які ініціативи Білого дому, спрямовані на підвищення кібербезпеки, не здійснюватимуться за рахунок обмеження громадянських свобод. 24 червня 2009 р. міністр оборони США Р. Гейтс заявив[10], що вже до жовтня 2009 р. у структурі Міністерства оборони буде створено Кіберкомандування США (*U. S. Cyber Command*). Попередньо очолити цю структуру має генерал К. Б. Александер – керівник Агентства національної безпеки, що свідчить про надзвичайно серйозну увагу з боку нової Адміністрації.

У контексті посилення кібербезпеки керівництво США зосереджено на величезній активності кіберзлочинців з Китаю, Північної Кореї та Російської Федерації. Останні викликають особливу занепокоєність у ФБР – на конференції *Black Hat*[11] представники ФБР та компанії *McAfee* присвятили виступи російським кіберзлочинцям, яких назвали "найбільш організованими та небезпечними з усіх"[12]. Ще в лютому 2009 р. з метою запобігання можливості "зламу" урядових комп'ютерних мереж було розширено повноваження Агентства національної безпеки США щодо контролю над кіберпростором США (у тому числі з можливістю втручатись у мережеві підсистеми федеральних та місцевих адміністрацій).

Загроза з боку китайських хакерів (які переважно працюють на уряд країни) стала вже звичною для американських та південнокорейських спецслужб. Так, у доповіді, оприлюдненій 31 березня 2009 р. у мережевому виданні одного з університетів Торонто (Мунк), стверджується, що розкрито операцію китайських спецслужб, найбільшу за всю історію кіберрозвідки, й детально описано її механізми. Йдеться про програму широкого спектра дії, яка, крім функції надсилання й одержання файлів, дає можливість підключати до комп'ютера відео- і аудіоприлади, щоб стежити за користувачами комп'ютерів.

Це був не перший зареєстрований випадок, коли Китай звинувачують у шпигунстві з використанням кібератак та шпигунського програмного забезпечення. У серпні 2007 р. журнал *Spiegel* звинуватив Китай у шпигунській кібератаці на уряд Німеччини, а у червні 2007 р. китайські військові "зламали" комп'ютерну мережу Пентагону (офіційно підтверджено керівництвом Міністерства оборони США).

Значну увагу використанню мережі Інтернет метою приділяє керівництво Північної Кореї. 4 липня 2009 р. сайти декількох американських та південнокорейських міністерств і відомств (зокрема, Міністерства фінансів, Секретної служби США, Пентагону, Федеральної торговельної комісії, Міністерства

---

[10] *Gates* Establishes New Cyber Subcommand [Електронний ресурс]. – Режим доступу : http://www.defenselink.mil//news/newsarticle.aspx?id=54890

[11] Перша конференція *Black Hat* відбулась у Лас-Вегасі в 1997 р. Її мета полягала в об'єднанні розробників систем безпеки та хакерів. Ця конференція швидко набула репутації головного зльоту хакерів. На заходах *Black Hat* проводяться семінари, на яких роз'яснюються засоби, використовувані хакерами для власного збагачення. Останнім часом майже на всіх конференціях *Black Hat* присутні представники спецслужб США.

[12] *Киберпреступники* из России – самые организованные и опасные, считают в ФБР [Електронний ресурс]. – Режим доступу : http://hitech.newsru.com/article/31jul2009/fbi

транспорту) були піддані масованій кібератаці, що призвела до відключень цих порталів на кілька днів. За даними південнокорейської розвідки, за цими атаками стояв спеціальний підрозділ, створений у Північній Кореї для вчинення кібератак[13]. Керівництво Південної Кореї ухвалило рішення про створення до 2012 р. окремого командування, що має захистити комп'ютерні мережі збройних сил від кібератак хакерів. Під час семінару з питань безпеки комп'ютерних мереж у Сеулі на початку липня 2009 р. представник Міністерства оборони Південної Кореї зазначив, що "кожного дня на сайти та у мережі відомства вчинюється 15 тис. хакерських та 80 тис. вірусних атак, причому 11 % з них є цілеспрямованими спробами отримати секретну інформацію"[14].

Тенденція до виокремлення спеціальних структур для протидії кіберзлочинності та кіберзагрозам поширюється і в європейських країнах. Велика Британія створила[15] в складі Кабінету міністрів Центральне управління з кібербезпеки (*The UK Central Office of Cyber Security – OCS*) й окрему структуру військового типу – Центр операцій з кібербезпеки (*UK Cyber Security Operations Centre*), який, подібно до аналогічної американської структури, здійснюватиме як оборонні, так і наступальні операції в кіберпросторі. У новому офісі працюватимуть співробітники трьох відомств – оборонного, розвідувального й правоохоронного, які будуть здійснювати моніторинг інформаційного простору та визначати своєчасні заходи реагування на різноманітні загрози й виклики.

Водночас ЄС поки що не відреагував на посилення кіберзагроз створенням нових міждержавних організаційних одиниць і залишає боротьбу з кіберзлочинами в компетенції національних урядів, хоча, згідно з опитуванням компанії *IPSOS* у червні 2008 р., практично кожен п'ятий європеєць, що користується Інтернетом, зазнавав шкоди від кіберзлочинців[16]. Найактивнішу політику у сфері регулювання кіберпростору (крім Великої Британії) наразі проводить Німеччина, в якій створено кіберполіцію[17].

Особливу увагу кібербезпеці та протидії кіберзлочинності приділяє НАТО. У п. 49 Декларації, прийнятій під час саміту НАТО, зазначається[18], що "комунікаційні та інформаційні системи є критично важливими для Альянсу". Підтверджується прагнення до "посилення їх безпеки з метою захисту від кібератак, як з боку державних, так і недержавних акторів". Для забезпечення цієї позиції країни НАТО погодилися на створення "центру кібероборони" (*NATO Cyber Defence Management Authority*), що має на меті вдосконалити наявну "можливість відповіді на комп'ютерні інциденти". Відповідно до Декларації кібербезпека НАТО має стати "інтегральною частиною структури НАТО", а крім того,

---

[13] *Специалисты* начали сомневаться в причастности Северной Кореи к кибератакам на правительственные сети США 4 июля [Електронний ресурс]. – Режим доступу : http://hitech.newsru.com/article/09jul2009/whodunnit

[14] *Вслед* за США собственное киберкомандование создает Южная Корея [Електронний ресурс]. – Режим доступу : http://hitech.newsru.com/article/30jun2009/rkcybercommand

[15] *В Великобритании* начнет работать центр кибербезопасности [Електронний ресурс]. – Режим доступу : http://www.securitylab.ru/news/381959.php

[16] *Каждый* пятый европеец пострадал от киберпреступников [Електронний ресурс]. – Режим доступу : http://www.securitylab.ru/news/354837.php

[17] *В Германии* увеличат число киберполицейских [Електронний ресурс]. – Режим доступу http://www.securitylab.ru/news/383708.php

[18] *Strasbourg* / Kehl Summit Declaration [Електронний ресурс]. – Режим доступу http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease

ця система повинна охопити не лише країни – члени НАТО, а й країни-партнери задля захисту їх від кібератак. З цією метою пропонується активізувати роботу Спільного кібербезпекового центру (*Cooperative Cyber Defence Centre of Excellence*) в Естонії.

В Україні дотепер захист кіберпростору забезпечується спеціальними департаментами різноманітних безпекових структур – Служби безпеки України, Служби зовнішньої розвідки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства внутрішніх справ України тощо. Водночас їх діяльність не завжди скоординована, а сфери відповідальності повністю не узгоджені. Все це може ускладнити реагування на потенційні кібератаки проти державних комп'ютерних мереж і сайтів у разі можливої міждержавної конфліктної ситуації або діяльності в національному сегменті кіберпростору терористичних груп.

Отже, ключовим світовим трендом у сфері кібербезпеки є формування спеціалізованих структур, що відповідатимуть не лише безпосередньо за захист кіберпростору, а й за розроблення наступальних технологій. Крім того, актуалізується тенденція (на прикладі США) введення посад спеціальних радників з проблем кібербезпеки. Можна прогнозувати, що проблема кібербезпеки залишатиметься однією з ключових для нової Адміністрації впродовж найближчих років. У США та ЄС посилюються контроль і моніторинг мережі Інтернет, що свідчить про поступове переосмислення ліберальних поглядів на мережу як на звичайний "простір вільного обміну думками".

Підбиваючи підсумки, зауважимо, що більшість *IT*-розвинених держав світу виокремлює як головних "порушників спокою" кіберпростору Китай, Північну Корею та Російську Федерацію. Європейський Союз залишається відносно інертним щодо вирішення проблеми безпеки власного кіберпростору, хоч окремі країни ЄС (Велика Британія, Німеччина) активно розробляють власну політику в цьому напрямі. Частково така інертність може бути пов'язана з тим, що більшість країн ЄС є членами НАТО, де створено спеціальний орган для захисту кіберпростору і, таким чином, опосередковано забезпечується вирішення цієї проблеми для Євросоюзу.

У контексті зазначеного Україна має активізувати власну політику щодо забезпечення безпеки національного кіберпростору. З огляду на висвітлені світові тренди у цій сфері, доцільно створити спеціалізовану структуру, на яку покласти всю відповідальність не лише за забезпечення захисту національної інфраструктури, а й за розроблення власних наступальних технологій кібервійн. Така структура (можлива назва – "Національне агентство з безпеки кіберпростору") може бути створена за одним із двох принципів:

– комплексно реалізувати функції спеціальних комітетів чи служб, до яких буде передано відповідні підрозділи Служби безпеки України, Служби зовнішньої розвідки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства внутрішніх справ України та інших державних органів, що відповідають за безпеку інформаційної інфраструктури держави;

– відігравати роль міжвідомчого координаційного центру (міжвідомчої координаційної групи), що має на меті оптимізувати (як законодавчо, так і на рівні узгодження порядку дій у надзвичайних ситуаціях) зусилля українських

спецслужб у сфері захисту національного кіберпростору. Створення такої Міжвідомчої групи можливе на базі Апарату РНБО України, очолювати її може один з перших заступників Секретаря РНБО України. У будь-якому випадку до її роботи варто залучати висококваліфікованих фахівців із системи НАН України та Міністерства освіти і науки України.

До першочергових завдань такої структури має належати підготовка українського аналога американського "Огляду кібербезпекової політики" (*Cyberspace Policy Review*), що має на меті визначити об'єктивний стан забезпеченості безпеки національного кіберпростору та запропонувати конкретні шляхи його покращення (законодавчі, організаційні, фінансові тощо). Підготовка такого звіту має відбуватися щороку.

Доцільно також нормативно регламентувати можливість вжиття надзвичайних заходів контролю за національною інформаційною інфраструктурою та мережею Інтернет у період кризових ситуацій. Окрім того, зважаючи на тенденцію впровадження провідними державами світу організаційних заходів посилення кібербезпеки, в уряді слід запровадити посаду відповідального за проблеми реалізації державних *IT*-проектів та безпеки вітчизняного кіберпростору.

7.16. ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ ЗАГОСТРЕННЯ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА США І КИТАЮ В КІБЕРПРОСТОРІ

Власюк О. С., Ожеван М. А., Дубов Д. В. Матеріали до аналітичної довідки (Київ, НІПМБ, березень 2010 р.). *Публікується вперше.*

Масштабна мілітаризація кіберпростору, започаткована Китаєм та США (зокрема, за інформацією КНР, Пентагон уже нині вкладає в кіберзасоби ведення бойових дій та забезпечення власного кіберзахисту більше, ніж у традиційні види озброєнь), залучення до вирішення проблемних питань у цій сфері міністерств закордонних справ обох держав свідчать про реальність глобальної інформаційної війни, яка поки що перебуває на стадії протистояння, подібного до часів "холодної війни".

Такий стан речей впливатиме на глобальну безпеку, зокрема й України, за двома основними напрямами. По-перше, посилення заходів кіберзахисту та ускладнення можливості атак на фінансові й інформаційні ресурси провідних держав світу призведе до пошуку кримінальними та військовими структурами нових, менш захищених, об'єктів, якими можуть стати елементи української інформаційної (фінансової) інфраструктури. По-друге, недостатня обізнаність українських громадян з основами комп'ютерної безпеки, неналежна захищеність державних мереж, у яких циркулює значуща для національної безпеки урядова інформація, полегшують для хакерів формування стартових майданчиків кіберпростору (нових заражених ботнетів – мереж, що складаються з певної кількості хостів з автоматичним програмним забезпеченням) для вчинення кібернападів з "чужої території".

Крім того, стрімке якісне та кількісне зростання кіберзагроз, пов'язаних із криміналізацією і мілітаризацією кіберпростору, перестає бути проблемою комерційних компаній, що найбільше страждали донедавна від таких трендів. "Політизація" хакерської діяльності привертає увагу провідних країн до кіберозброєнь і "кібервоєн", переводить проблему на рівень державної та наддержавної безпеки.

Особливості американсько-китайського протистояння

Станом на 2009 р., за даними керівника компанії *McAfee*, оприлюдненими на Всесвітньому економічному форумі в Давосі у 2010 р., уже понад 20 країн планували здійснювати або реально здійснювали різноманітні інформаційні операції, спрямовані проти Сполучених Штатів. Формуються спецпідрозділи, які мають на меті ведення розвідувальної роботи в мережах, захист власних мереж, блокування та руйнування структур супротивника. За даними головного контрольно-фінансового управління Конгресу США за 2007 р., на той час уже принаймні 120 держав розпочали формування груп фахівців, які мали в майбутньому стати ядром для кібервійськ, з метою дослідження стратегії й тактики інформаційних війн. Китайські та російські кібервійська вважаються найактивнішими, реалізуючи постійні напади на мережі держав у всьому світі й особливо – на мережі США[19].

13 січня 2010 р. корпорація *Google* заявила, що покине китайський ринок, якщо не припиняться напади на її мережі китайських хакерів, які діють, на думку керівництва корпорації, з відома керівництва КНР. Ідеться нібито про злам електронних поштових скриньок, які належать китайським правозахисникам. Але насправді претензії *Google* та інших американських компаній стосуються не стільки прав людини, скільки прав самих компаній в інтелектуально-інформаційній сфері, оскільки для здобуття конкурентних переваг КНР вдається до масштабних акцій промислового шпигунства, організовуючи хакерські напади на внутрішні мережі іноземних компаній, сайти топ-менеджерів тощо[20].

Характерно, що під час з'ясування стосунків між корпорацією *Google* та керівництвом КНР вперше на захист інтересів бізнес-компанії став Державний департамент США. Це ще раз засвідчує серйозність намірів американського керівництва реалізувати у стислі терміни доктрину Барака Обами щодо захисту інформаційної інфраструктури США шляхом якомога тіснішої взаємодії представників бізнесу і влади, спільного ведення наступальних та оборонних

---

[19] Зростання хакерського потенціалу КНР пов'язане не лише з підтримкою такої діяльності керівництвом держави, а й з її економічною привабливістю. За даними, оприлюдненими китайською "Компанією комп'ютерної безпеки – 360", рівень доходів китайських хакерів у 2009 р. сягнув 1,5 млрд дол. США.

[20] Це вже не перша сутичка між корпорацією *Google* та органами цензури КНР, хоча до останнього часу проблеми вирішувались на двосторонньому рівні без залучення потужностей Державного департаменту США. Декілька років тому під тиском влади КНР *Google* погодився на певні обмеження, які діяли щодо китайських користувачів її пошукової системи, зокрема, на цензуру результатів пошуку, однак надалі між *Google* та китайською владою періодично виникали розбіжності щодо того, який контент має бути блоковано. У червні 2009 р. Пекін звинуватив *Google* у тому, що порнографічні ресурси не цензуруються, і тимчасово закрив доступ до ресурсів *Google.com* та *Gmail* (поштова служба *Google*).

інформаційних війн і забезпечення інтересів національної інформаційної безпеки. Ідеться про міжвідомчу "Всеосяжну ініціативу з національної кібербезпеки" (*Comprehensive National Cybersecurity Initiative*), спрямовану на захист Федеральної державної інформаційної інфраструктури від комп'ютерних загроз і нападів, яку запровадив президент Дж. Буш 8 січня 2008 р. і яка набула подальшого розвитку за президентства Б. Обами.

Важливість такого тотального захисту підтверджується в секретній доповіді ФБР щодо розвитку кібервійськ КНР та спричинених ними загроз національній безпеці США. В інформації, що просочилася з цієї доповіді, оприлюдненій у пресі в середині січня 2010 р., КНР названо "найбільшою цілісною загрозою США у сфері кібертероризму" та силою, яка наразі володіє потенціалом, що дає можливість "знищувати життєво важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних".

За даними доповіді, КНР має армію зі 180 тис. хакерів, які вчинюють постійні атаки на кібермережі США (лише у 2009 р. проти комп'ютерів Міністерства оборони США було вчинено 90 тис. таких атак). Згідно з даними ФБР зі 180 тис. кібершпигунів 30 тис. є військовими, а 150 тис. – комп'ютерними експертами з приватного сектору, місія яких полягає в отриманні доступу до військових і комерційних таємниць США та внесенні розладу в діяльність урядових і фінансових служб[21].

З метою залучення хакерів до військових підрозділів армії КНР діють комплексні програми пошуку обдарованої молоді. Урядові агенти Китаю проводять відповідну роботу в різних хакерських клубах, які фактично перетворилися на бази рекрутування молоді до військових кіберпідрозділів армії КНР[22]. Щоправда, цей підхід не оригінальний, оскільки тим самим шляхом ідуть США і ЄС. Водночас на власній території керівництво Китаю рішуче протидіє будь-якій хакерській активності організованих угруповань, які або не бажають співпрацювати з державними службами, або опосередковано підривають монополію держави на контроль за контентом, доступним китайським користувачам[23].

КНР ставить за мету створити до 2020 р. "найбільш інформатизовану" армію у світі. Основною інформаційною зброєю китайських хакерів є "шкідники" (англ. *malicious*) – заражені комп'ютерні коди. Вже у 2009 р. компанії, що здійснюють діяльність в енергетичній, банківській, аерокосмічній та телекомунікаційній сферах, мали суттєві проблеми з китайським "шкідливим" комп'ютерним кодом. Причому компанії із запізненням усвідомили масштаби та загрозу атак, започаткованих ще у 2008 р., і попередили ФБР про ці атаки лише на початку 2009 р. Тим часом китайські хакери, які використали принципово нові типи вірусів, що не визначалися жодним спеціальним антивірусним

---

[21] *China's* Secret Cyberterrorism [Електронний ресурс]. – Режим доступу : http://www.thedailybeast.com/blogs-and-stories/2010–01–13/chinas-secret-cyber-terrorism/full

[22] Докладнішу інформацію про типовий механізм залучення молодих китайських *IT*-спеціалістів до кіберпідрозділів армії КНР див. : *The United* States Cyber Challenge. – Ch. 1 [Електронний ресурс]. – Режим доступу : http://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1 %20 %28updated%205–8–09 %29.pdf

[23] *Закрыта* крупнейшая школа хакеров в Китае [Електронний ресурс]. – Режим доступу : http://www.3dnews.ru/news/zakrita_krupneishaya_shkola_hakerov_kitaya

програмним забезпеченням, отримали доступ до найважливішої комерційної інформації, у тому числі до результатів розвідки територій, електронного листування топ-менеджерів компаній тощо.

Ефективною є діяльність китайських хакерів проти військових баз даних Пентагону. Найрезонанснішим був напад у червні 2007 р., коли китайським хакерам вдалося отримати доступ до комп'ютерної мережі Пентагону, і, відповідно, – до внутрішнього електронного листування співробітників та порушити роботу близько 1500 комп'ютерів військового відомства[24].

На початку 2009 р. американські військові підтвердили нові факти зламу інформаційної бази Пентагону[25]. Хакери спромоглися зняти декілька терабайт інформації щодо новітніх розробок ВПС США (ідеться, зокрема, про розробки винищувачів нового покоління, бюджет яких становить близько 300 млрд дол. США).

Останньою ефективною атакою хакерів, вчиненою, за версією Міністерства оборони США, спецпідрозділами Північної Кореї за безпосередньої підтримки хакерів з КНР, є викрадення з комп'ютерів Міністерства оборони Південної Кореї оперативних планів розгортання американських військ на території півострова у випадку конфлікту з КНДР.

Справжні масштаби кібератак набагато серйозніші. Те, що оприлюднюють медіа, є незначним просоченням резонансної інформації, яка має привернути увагу громадськості до цієї проблеми, щоб організувати лобіювання в Конгресі США прийняття дедалі дорожчих програм кіберзахисту.

Зокрема, у відповідь на посилення позицій Китаю в кіберпросторі Пентагон нарощує зусилля з протидії засобам кібервійн. Триває процес оновлення Агентства оборонних перспективних дослідницьких проектів (*DARPA*), на замовлення якого свого часу було створено *Arpanet*, що згодом перетворився на сучасний Інтернет. Нині Агентство започаткувало проект *National Cyber Range* (*NCR*), пов'язаний з розробленням програми, яка дасть можливість в оперативнішому режимі й більш системно оцінювати готовність національних інформаційних мереж до відбиття хакерських нападів. Мета програми *NCR* – "революціонізувати сучасні кібертехнології тестування нападів", а також "забезпечення всеосяжної, якісної і кількісної оцінки безпеки інформаційних та автоматизованих систем контролю", які перебувають поки що на стадії розроблення.

DARPA уклала контракт з *Lockheed Martin* (орієнтовна сума – 31 млн дол. США) на створення нової версії Інтернету для військових цілей з новим протоколом під кодовою назвою *Military Network Protocol* (*MNP*), що має забезпечити підвищену безпеку та динамічний перерозподіл пропускної здатності каналів навіть в умовах масованих кібератак.

Китайська сторона небезпідставно звинувачує американців у тому, що не Китай, а США вперше спроектували й реалізували концепцію "кібервійськ", а американська розвідка може за допомогою спецзасобів здійснювати моніторинг

---

[24] *Китайцы* взломали Пентагон [Електронний ресурс]. – Режим доступу : http://www.itsec.ru/newstext.php?news_id=34060.

[25] *Хакеры* взломали доступ к самому дорогому проекту Пентагона [Електронний ресурс]. – Режим доступу : http://top.rbc.ru/society/21/04/2009/295893.shtml

онлайнової інформації, яка шкодить національним інтересам США, та знищувати її. Тому "за такої політики було б цілковитим безглуздям вимагати від інших країн забезпечення вільних потоків інформації в мережі"[26].

КНР, безумовно, має рацію в тому, що США, які вперто намагаються зберегти лідерство у сфері найпередовіших ІКТ, відмовляються долучатися до переговорного процесу під егідою ООН щодо впорядкування (або повної заборони) використання кіберозброєнь та протидії мілітаризації кіберпростору. Проте, за деякими повідомленнями, певні позитивні зрушення в цьому процесі вже є[27].

Очевидно, що мілітаризація кіберпростору вже в найближчому майбутньому сягне критичної позначки, коли виникнуть об'єктивні передумови для укладання на міжнародному рівні спеціальних регулюючих договорів з питань інформаційної безпеки та оборони. Подібні договори з міжнародної інформаційної безпеки, ініційовані ще в 1990-х рр. РФ та КНР, поки що вперто торпедуються США. Проте неможливість забезпечити власне лідерство у сфері ІКТ і вразливість до численних кібернападів змусять США піти на поступки в питаннях укладання договору з міжнародної інформаційної безпеки, який прирівняє інформаційну зброю до зброї масового ураження та заборонить на рівні міжнародного права її "проліферацію".

Україна як повноправний член ООН повинна повною мірою долучитися до діалогу щодо підготовки масштабного міжнародного договору з питань нерозповсюдження інформаційної зброї, боротьби з кібертероризмом та шпигунством в Інтернет-просторі. Доцільно активізувати роботу у форматі комісій, експертних груп, інших дорадчих та координуючих органів ООН, задіяних у виробленні політики ООН у сфері міжнародної інформаційної безпеки та глобальної кібербезпеки. Варто також ініціювати обговорення питань кібербезпеки в рамках як двосторонніх українсько-російських відносин, так і співробітництва України з міжнародними організаціями – Вишеградською групою, ЄС, НАТО, ОДЕР – ГУАМ, ОЧЕС.

Слід зазначити, що у розвинених країнах світу є потужні програми пошуку, мотивації та підтримки "інформаційно обдарованої" молоді. Це забезпечує їм домінуючі позиції на ринку кіберозброєнь як у кількісному, так і в якісному вимірі. Аналогічної програми з належною бюджетною підтримкою потребує Україна. З метою посилення кібербезпеки та протидії кіберзлочинності слід детально вивчити і впровадити в Україні досвід діяльності Центру міжнародного багатостороннього партнерства проти кіберзагроз та Центру глобальної відсічі в кіберпросторі.

Україні необхідно переглянути політику кіберінформаційної безпеки передусім у соціогуманітарному вимірі, зупинивши з допомогою моральних та матеріальних стимулів відплив з України висококваліфікованих фахівців з ІКТ. За прикладом високорозвинених країн слід розробити та реально втілювати в життя програму добору, моніторингу й супроводу обдарованої у сфері точних наук та комп'ютерних технологій молоді. Необхідно взяти під особливий

---

[26] Цит. за : *China* Accuses US of Using Cyberwarfare [Електронний ресурс]. – Режим доступу : http://www.ft.com/cms/s/0/092d5ab6-08fc-11df-ba88-00144feabdc0.html?nclick_check=1

[27] *Россия* и США обсуждают кибербезопасность [Електронний ресурс]. – Режим доступу : http://www.cybersecurity.ru/armament/83820.html

контроль уповноважених державних інспекторів школи, комп'ютерні клуби тощо для залучення такої молоді до розроблення й підтримки програм безпеки кіберінформаційного простору.

З урахуванням міжнародного досвіду Україні слід започаткувати створення кібервійськ. Для цього необхідно забезпечити відповідну нормативно-правову базу, внести зміни до Закону України "Про оборону України", до Воєнної доктрини України, Стратегії національної безпеки, Доктрини інформаційної безпеки та Концепції державної інформаційної політики України. Такі зміни мають розставити необхідні акценти на питаннях посилення кіберскладника національної безпеки і оборони та забезпечити правове підґрунтя становлення, розвитку й захисту національної воєнно-інформаційної інфраструктури.

7.17. ДО ПИТАННЯ МОДЕРНІЗАЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

Власюк О. С. Матеріали до виступу на V Науково-практичній конференції "Актуальні проблеми управління інформаційною безпекою держави" (Київ, Академія Служби безпеки України, 19 березня 2015 р.). *Публікується вперше.*

Проблема управління інформаційною безпекою держави є сьогодні однією з найбільш актуальних. Її доцільно окреслити в більш широкому контексті управління системами безпеки та оборони в складні часи, які переживає нині Українська Держава, коли кинуто виклик її існуванню як незалежної держави і коли доводиться прощатися з багатьма ілюзіями.

Одна з цих ілюзій стосувалася ймовірної війни з Росією. Більшість із нас відкидала цю ймовірність за принципом тотальної безпечності – "цього не може бути, бо цього не може бути ніколи".

Сучасна криза – як загальносвітова, так і українська – позначена передусім кризою керованості й управління у всіх формах та на всіх рівнях. Застарілі, вертикально-інтегровані схеми управління або взагалі не працюють, або працюють вкрай неефективно. З новими мережевими підходами до управління теж виникає чимало проблем.

Особливо усе це стосується державного правління. Українській Державі нині кидають виклик не лише зовнішні й внутрішні опоненти та відверті вороги, а й низка тіньових та напівтіньових структур, які підживлюють міжнародну і внутрішню злочинність, тероризм, сепаратизм тощо.

Першопричиною втрати країнами національно-державного суверенітету є інформаційна бідність або ж втрата інформаційного суверенітету, і це, напевно, – центральна проблема інформаційної безпеки, якщо це поняття не звужувати до захисту інформації чи регулювання діяльності масмедіа.

Дедалі частіше до низки сучасних держав застосовується термін "неспроможні держави", "держави, що не відбулися" (*failed states*). Як відомо, наші кремлівські недруги охоче вживають подібну термінологію стосовно України, явно видаючи бажане за дійсне. І це теж питання інформаційної безпеки. Навіть цілі регіони земної кулі нині сприймаються у міжнародних колах під кутом зору "вакууму безпеки".

Так або інакше, мусимо констатувати кризу розуміння ключових понять "безпека" й "національна безпека", пов'язану, по-перше, з тим, що істотно розширилося коло суб'єктів та об'єктів безпеки, а, по-друге, інформаційна революція дала змогу збагнути таку кількість ризиків, викликів і загроз для безпеки на всіх її рівнях та у всіх її різновидах, що це складне "мереживо" часто не піддається раціональному осмисленню. Звідси виникає розуміння соціальної дійсності як керованого або некерованого хаосу.

Ідеться також і про конфлікт адміністративно-командних та ринково-маркетингових підходів до управління безпекою або менеджменту безпеки.

Наслідком зазначеного є необхідність ретельного добору пріоритетів безпеки, тобто проблем, які можуть за наявних ресурсів бути не просто задекларованими, а й реально вирішеними у короткостроковій, середньостроковій або довгостроковій перспективі. Саме тому у всьому світі посилюється тенденція до управління системами безпеки й оборони через управління ресурсами. Тобто йдеться не про декларування "благих намірів", а про визначення ресурсів, які або вже є в розпорядженні керівників вищого рівня у сфері оборони та безпеки, або їх необхідно надати у тимчасове користування для виконання певних завдань.

Особливого значення набуває програмне управління ресурсами у критичних надзвичайних ситуаціях, якою, безумовно, є Антитерористична операція, коли необхідно використовувати підходи, що максимально зближують поняття адміністрування або командування із творчим менеджментом, зусилля держави й волонтерських організацій.

Перше й найпростіше, що слід робити в теперішніх умовах, – це встановити якомога тісніші кореляції між вимогами безпекової та оборонної сфери й реальними можливостями державного бюджету. Але ще важливішим є взаємопогоджене розумінням майбутнього, до якого слід намагатися дійти в процесі розвитку безпекових та оборонних структур.

Отже, управління ресурсами безпеки та оборони перетворюється нині на інструмент оцінювання ефективності використання загальносуспільних фондів, починаючи від елементів інфраструктури, людських ресурсів і капітальних інвестицій у безпеку та оборону й закінчуючи періодичними витратами оперативного та експлуатаційного змісту.

На особливу увагу заслуговують інноваційний потенціал та інтелектуальні інвестиції у сфері безпеки й оборони, роль та значення яких в епоху інформаційної революції важко переоцінити. Ідеться передусім про мережевоцентричні чинники управління ресурсами, зорієнтовані на досягнення інформаційної переваги під час проведення різноманітних операцій безпекового або оборонно-воєнного характеру. Таке переважання досягається завдяки створенню комунікативної мережі розподілених центрів, що пов'язують між собою джерела інформації та засоби детекції з особами, що ухвалюють рішення, й виконавцями, які ці рішення реалізують. Тільки таким чином можна забезпечити своєчасне доведення до всіх учасників АТО інформації про реальну ситуацію.

Насамкінець хотів би зупинитися на принципових перешкодах на шляху впровадження сучасного інформаційного менеджменту в українських умовах.

Перша й найголовніша для нашого соціуму перешкода полягає у непрозорості процесів формування та витрачання ресурсів, у відсутності належної

достовірної інформації, доступної для всіх учасників процесу планування і програмування. Подібна непрозорість (нетранспарентність) живить корупцію, але й корупція, у свою чергу, культивує подібну непрозорість. Є ще й така перешкода, як культура надмірного втаємничування, наслідком якої є недоступність інформації безпекового або оборонного змісту для всіх учасників процесу планування та програмування, особливо тих, які представляють цивільний і комерційний сектори економіки, волонтерські організації тощо.

Не слід забувати й про те, що програмування розвитку безпекової та оборонної сфери – це підходи, перенесені зі сфери ринкового бізнесу, де учасники комерційних процесів звикли рахувати кожну копійку. Так і має бути в безпековій та оборонній сферах. В умовах СРСР, де вся економіка фактично працювала на безпеку та оборону, вважалося, що безпеку не слід комерціалізувати й на неї не слід поширювати ринкові підходи та оцінки. Коли такий підхід було перенесено на умови незалежної України, то склалася парадоксальна ситуація, коли Міністерство оборони та інші структури, які представляють воєнну організацію держави, маючи значні матеріальні ресурси, фактично не могли розпоряджатися ними, а коштів самого міністерства ледве вистачало на виплату зарплат офіцерам та на харчування солдат.

Аналогічна ситуація була з іншими міністерствами та відомствами так званого силового блоку. При цьому більшість моделей менеджменту сектору безпеки і оборони наших західних партнерів будується на принципово інших основах, відмінних від радянських та пострадянських моделей.

Цю негативну тенденцію розвитку оборонно-безпекового сегмента державного управління досі не вдається подолати, унаслідок чого система національної безпеки й оборони України нині переживає важкі випробування, починаючи з питань кадрових і закінчуючи питаннями фінансовими, техніко-технологічними тощо.

Зазначена проблема стосується не лише класичних "матеріальних" складників сектору безпеки і оборони, а й таких, як інформаційна безпека. Тут також моделі інформаційної безпеки держави будувалися без урахування реальних матеріальних ресурсів та можливостей суспільства. Відповідно, сфера інформаційної безпеки держави має бути піддана такій самій трансформації моделі менеджменту, як і вся система національної безпеки.

У цьому контексті особливої ваги набувають практично придатні критеріальні оцінки щодо ефективності організації та функціонування інститутів безпеки й оборони та щодо ролі експертних напрацювань у процесі підготовки, ухвалення й імплементації державних рішень у системі національної безпеки та оборони України. Ідеться також про критеріальні оцінки виконання самих рішень, а також пов'язаних із ними ризиків, викликів та загроз.

Забезпечення інформаційної безпеки сьогодні вимагає пошуку перспективних шляхів тісної взаємодії й координації державних та недержавних структур у системі національної безпеки, що нині позначається терміном "приватно-публічне партнерство". Не секрет, що рішення у сфері інформаційної безпеки на рівні держави, структур громадянського суспільства та бізнесу доволі часто є надто суперечливими, а їх реалізація не завжди відбувається у цивілізований спосіб.

Важливим способом погодження інтересів, взаємозв'язку і взаємодії державних та недержавних структур є діяльність аналітичних центрів (*think tanks*), задіяних у процесі підготовки, ухвалення й імплементації безпекових рішень в Україні.

Отже, актуалізується низка питань щодо національної політики імплементації рішень, труднощів забезпечення їх збалансованості та об'єктивності в умовах як надмірної інформаційної закритості, так і надмірної відкритості владних структур. При цьому ключовою передумовою успішної імплементації рішень у системі національної та інформаційної безпеки є необхідність єднання навколо цього питання інтелектуальної, економічної і політичної еліт, держави та суспільства, держави й бізнесу.

7.18. ПРАВА ЛЮДИНИ ТА ВИКЛИКИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Власюк О. С. Виступ на науково-практичній конференції "Проблеми захисту прав людини в інформаційному суспільстві" (Київ, НТКУ "Київський політехнічний інститут", 1 квітня 2016 р.). *Публікується вперше.*

Проблематика захисту прав людини в умовах інформаційного суспільства не просто "актуальна" чи, як кажуть, "на часі". Насправді потреба її вирішувати значно випереджає нашу готовність це робити. Права людини, їх захист – це безумовні надбання розвинених демократичних суспільств. Власне, їх дотримання – це основа нашої цивілізації. Однак стрімкий розвиток інформаційних технологій та становлення інформаційного суспільства зумовлюють надзвичайно складні виклики в цій царині. Поступовий рух людства через розвиток технологій уже сьогодні ставить питання: якою мірою ми взагалі маємо розуміти права людини?; чи будуть вони залишатися такими, якими ми їх звикли розуміти?; як їх захистити в цьому новому світі?

Інформаційне суспільство глибоко трансформує наше уявлення про більшість класичних прав людини, про які ми зазвичай говоримо. Ідеться про те, що ми перестаємо їх визнавати. Однак сам формат їх розуміння змінюється. Цікаво, що суть проблеми сьогодення досить чітко сформулював ще у XIX ст. британський економіст та філософ Джон Стюарт Мілл: "Якщо ми називаємо щось правом людини, ми маємо на увазі, що вона обґрунтовано претендує на свій захист з боку суспільства у своїй можливості володіти цим правом, силою закону, або через освіту і формування суспільної думки".

Однак саме в питаннях володіння цим правом та його захисту з боку суспільства чи держави ми і стикаємось сьогодні з найбільшими загрозами та небезпеками. Безумовно, йдеться не про всі права, закріплені Декларацією прав людини. Однак ключові з них, безумовно, опиняються під тиском поточного розвитку суспільства та його технологічного складника. Ідеться про:

– статтю 3, згідно з якою "Кожна людина має право на життя, на свободу і на особисту недоторканність";

– статтю 12, відповідно до якої "Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань";

– статтю 19, згідно з якою "Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів".

Насправді в цих питаннях ми все ще міркуємо категоріями середини XX ст. Ми все ще оперуємо реальністю, якої більше немає. І в цій уявній реальності саме держава є:

– по-перше, основним утримувачем знань про своїх громадян;

– по-друге, монопольно володіє цим знанням і може їм розпоряджатися:

– по-третє, захищає ці знання (або інформацію) і гарантує її збереження від посягань.

Однак реальність змінилася. Так само як сьогодні ми кажемо про "гібридну агресію", ми вже можемо говорити і про своєрідне "гібридне право" або "гібридні суверенітети" держав.

Чому "гібридні"?

Бо нині насправді не держава володіє повною інформацією про людину, а приватні корпорації, які мають виняткові можливості збирати, обробляти та використовувати персональні дані громадян. Тим самим вони прямо чи опосередковано порушують їх права у власних інтересах. Однак при цьому саме від держави як від єдиного офіційного суб'єкта міжнародних відносин, що відповідає за безпеку та захист прав громадян, вимагають захистити ці права, які часто порушуються навіть не нею. Більше того, ці права часто порушуються через недбале ставлення до них самих громадян.

Так, держави мають можливість використати свої ресурси та права для захисту традиційних прав людини і громадянина. Водночас ми всі повинні чітко зрозуміти, що це матиме всі риси своєрідного "неолуддизму", фактично боротьби проти сучасних технологій. І, до речі, цим шляхом окремі держави таки йдуть. Як це виглядає у найбільш рафінованому вигляді, можна побачити на прикладі Північної Кореї, де мобільний зв'язок та Інтернет – лише для обраних. При цьому сама держава настільки масштабно порушує права своїх громадян у всіх сферах, що насправді складно сказати, від чого проблем більше – від держави чи від потенційної небезпеки порушення прав людини з боку недержавних гравців. Тож виникає своєрідна дилема: заходи із захисту прав людини в інформаційному суспільстві можуть супроводжуватися власне порушенням цих прав.

За великим рахунком йдеться про необхідність вироблення нових глобальних правил гри для всіх учасників цього процесу. Маємо чітко говорити, що традиційні "права людини" є незмінними. Однак форми і масштаби їх забезпечення – це питання серйозних фахових дискусій.

Держава не може зробити вигляд, що не помічає ситуації, яка склалася. Несанкціонований збір персональних даних, їх постійні витоки, несанкціоноване втручання у приватне життя, розвиток технологій аналізу "Великих даних" *(Big Data*) – вже сьогодні це робить людину майже беззахисною перед глобалізованим інформаційним простором. Чим далі, тим більше люди наближаються до тієї самої точки сингулярності, про яку як про невідворотне майбутнє людства говорять трансгуманісти. Рівень присутності людей (а отже, інформації про них) у відкритих телекомунікаційних мережах надзвичайний. Мережі зв'язку стали