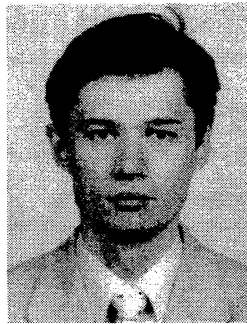


**ГУМЕНЮК Б.І.,
доктор історичних наук,
професор, ректор**

*Дипломатична
академія України
при МЗС України*



**ЩЕРБА О.В.,
кандидат політичних
наук**

*Інститут міжнародних
відносин Київського
національного
університету
імені Тараса Шевченка*

НОВА СИТУАЦІЯ У СВІТІ І ДИПЛОМАТІЯ

Дипломатична служба за своєю природою особливо вразлива до будь-яких нових відкриттів чи технічних винаходів. Варто згадати, як прискорився темп роботи дипломата в ХІХ ст. після того, як атрибутом повсякдення стали залізниці, що надало дипломатам можливість мобільно пересуватися між державами та по країні перебування.

Іншою поворотною подією стало відкриття електричного телеграфу, яке значно розширило можливості обміну інформацією між центром та закордонними представництвами. На думку ряду експертів, це був сумний день для дипломатії, оскільки прискорення інформаційних сполучень суттєво знизило автономність посольств від центру. Натомість інші дослідники (наприклад, Даглас Баск) вважають, що відсутність вчасних інструкцій,

як правило, ще більше зв'язувала ініціативу послів за кордоном, які більш за все боялися зробити помилковий крок.

Як би там не було, з моменту винайдення телеграфу закордонне представництво стало більшою мірою виконавцем, ніж співавтором політичних рішень. Причетність дипломата до їх прийняття знизилась і надалі знижалася в міру зростання оперативності та регулярності контактів на рівні центр – закордонна місія.

Аналогічно, як зазначалося вище, подальший розвиток телефонного зв'язку, радіо, телебачення, супутникових систем наклав відбиток на темп і специфіку дипломатичної діяльності.

А втім, жоден з цих чинників не справив фундаментального впливу на природу дипломатичної діяльності. На початку нового сторіччя ми маємо справу з новою ситуацією, коли бурхливий розвиток комп'ютерних, цифрових технологій приводить до кардинальних змін у двох сферах людської життєдіяльності, які завжди були стовпами, основою дипломатичної діяльності: комунікації та інформації. Далі ми спробуємо насамперед дослідити, в яких сферах дипломатії застосування інформаційних технологій (ІТ) уже тепер виправдовує себе, і які наслідки ці процеси можуть мати для дипломатичного фаху як такого, в тому числі в Україні.

Спочатку наведемо результати дослідження, проведеного в Гарвардському університеті, яке передбачило для приватних компаній таку градацію залежно від рівня застосування інформаційних технологій:

Стратегічна група (strategic group), тобто фірми, для яких безпроблемне функціонування інформаційних мереж має ключове, стратегічне значення.

Переломна група (turnaround group), тобто фірми, де успіх безпосередньо не залежить від ефективного використання комп'ютерної техніки, але застосування нових можливостей має життєве значення на перспективу.

Фабрична група (factory group), тобто підприємства, які використовують інформаційні технології для заощадження коштів і забезпечення безперебійної діяльності, але більше зацікавлені у збереженні наявних комп'ютерних систем, аніж у їхньому оновленні.

Другорядна група (support group), тобто фірми, для яких використання інформаційних технологій не має ключового значення¹.

Було б некоректним проводити тут повну паралель з діяльністю державних установ, проте певною мірою цю градацію можна застосувати і щодо них. Оскільки постійне і безперебійне надходження інформації з закордонних місій та інших джерел до міністерства закордонних справ є принципово важливим для виконання його основних завдань, МЗС має бути зараховане принаймні до другої, "переломної" групи. При цьому, досвід міністерств закордонних справ

провідних західних країн міжнародних організацій та NGO's дає підстави стверджувати, що місце МЗС та інших дипломатичних установ – уже не в другій, а в "стратегічній", першій групі.

Інформаційні технології дедалі більше перетворюються на інструмент політичного впливу. Миттєве розповсюдження новин в Інтернеті означає, що в МЗС мають працювати, збирати і розповсюджувати інформацію швидше, ніж у минулому, аби постійно тримати політичне керівництво країни в курсі подій та робити своєчасні рекомендації щодо реагування на ту чи іншу подію.

Інформаційні системи, маючи на увазі, насамперед, внутрішні комп'ютерні мережі, мають значний потенціал на виконання дипломатією її повсякденних завдань, зокрема адміністративну діяльність, захист економічних інтересів, зв'язки з громадськістю, консульську роботу тощо.

Використання ІТ полегшує виконання міністерством його координуючих функцій у міру того, як інші державні установи чимраз більше залучаються до діяльності на міжнародній арені. Комп'ютерна мережа створює можливості для безперервного спілкування МЗС з іншими установами, надання міністерству закордонних справ оперативної інформації.

Більшість міністерств закордонних справ на даному етапі стоїть перед необхідністю заощадження бюджетних коштів. Інформаційні технології дають змогу досягнути кращого результату за меншої собівартості. Нижче це буде продемонстровано на прикладі проєктів, здійснених останніми роками в МЗС ФРН та Державному департаменті США.

Починаючи з 1993 р. відбувся якісний стрибок у використанні комп'ютерної техніки дипломатичними службами світу. Досить сказати, що вже в 1993 р. той же британський Форін Офіс одержав премію британської промисловості за нову комп'ютерну мережу, запроваджену в міністерстві². Станом на 1999 р. 16,4% усіх британських дипломатичних та консульських місій мали власні веб-сайти та були об'єднані між собою в мережу. Ця система, як і аналогічні мережі в європейських МЗС, забезпечила автоматизацію документообігу та комунікації в рамках міністерства.

В 1992 р. Держдепартамент Сполучених Штатів уперше почав розповсюджувати в електронному вигляді на комп'ютерних компакт-дисках підшивку циркулярних листів, які регулюють діяльність міністерства та закордонних місій (багатотомне видання, на роздрук і розсилання якого закордонним установам щороку витрачалися значні кошти). Як виявилось, собівартість одного компакт-диску який містить увесь обсяг інформації, що потребував раніше багатьох томів, становить два дол. Щорічне заощадження склало 500 тис.

дол. Крім фінансової вигоди, перехід на використання електронної бази даних мав і численні інші переваги. На відміну від друкованого варіанта, який випускався щорічно, він підлягає щоквартальній актуалізації й містить повну базу даних з американської дипломатичної служби, порівняно просту в користуванні. Нині Держдепартамент практично повністю припинив випуск підшивок циркулярних листів у друкованому вигляді³.

Іншим цікавим прикладом заощадження коштів МЗС завдяки активному запровадженню інформаційних технологій є системи фінансово-адміністративного контролінгу що вже тривалий час функціонують у дипломатичних службах Великої Британії, Франції, Австрії, Швейцарії та Нової Зеландії.

Зупинимося коротко на такому проекті, який нещодавно пройшов успішну апробацію в МЗС ФРН.

У 1995 р. в одному з аналітичних листів ЦРУ так звана кібернетична війна була поставлена за рівнем небезпечності для американських національних інтересів на четверте місце після застосування атомної, біологічної та хімічної зброї. Та обставина, що в економіці, промисловості, фінансово-банківських системах держав світу дедалі ширше застосовуються новітні інформаційні технології, робить людське суспільство більш вразливим для небезпек, пов'язаних з використанням комп'ютерів.

2000 рік став особливо показовим у цьому плані. Досить згадати панічні прогнози щодо глобального падіння комп'ютерних систем внаслідок так званої "проблеми 2000", які, на щастя, не виправдалися. Але минуло п'ять місяців, і 4 травня понад мільйон комп'ютерів по всьому світові, навіть в урядових структурах, включаючи Пентагон, стали жертвами вірусної атаки, спричиненої, як вважається, школярем-вундеркіндом з Філіппін. Коментуючи цю вражаючу подію на сторінках "Ді Вельт" голова найбільшого у світі концерну-виробника систем комп'ютерної безпеки в глобальній комп'ютерній мережі Computer Associates Чарльз Б. Венг заявив: "Те, що відбувається нині в Інтернеті можна порівняти з часами, коли на вулицях міст з'явилися перші автомобілі. Тоді теж ніхто не думав про світлофори, розмітку чи знаки "стоп". Проте нині спільним завданням промисловості та урядів є потурбуватися про більшу безпеку в Інтернеті".

Міркування безпеки і захисту інформації традиційно мають для МЗС особливо вагоме значення. Регулярно працюючи з конфіденційними чи навіть таємними документами, воно має забезпечувати їм відповідний захист, навіть передаючи їх до найбільш віддалених регіонів світу.

Дещо спрощуючи, вимоги безпеки зводяться до забезпечення можливості зробити інформацію недосяжною в разі недозволеного втручання та захистити її від вірусів. З огляду на цю вимогу більшість сучасних

міністерств закордонних справ не підключають свої внутрішні мережі Інтернету чи інших відкритих інформаційних систем⁴.

Для міністерств закордонних справ характерна загальна тенденція до зниження кількості так званих захищених документів. Держдепартамент Сполучених Штатів оприлюднив інформацію, згідно з якою за період між липнем 1973 р. та лютим 1993 р. 72,8% усіх документів не заслуговували жодного грифа. 10,3% отримали найнижчу категорію секретності – "for limited official use" 13,1% документів мали конфіденційний характер ("confidential") 3,8% були секретними ("secret") та 0,02% – суворо секретними ("top secret")⁵. Аналогічні дослідження проведено в інших міністерствах закордонних справ. Так, британський дослідник С. Ілдон, не називаючи країни, повідомляє, що в одному з інших західних МЗС у результаті таких підрахунків з'ясувалось, що 94% усієї підготовленої міністерством інформації або взагалі мають відкритий характер, або підлягають лише елементарному захистові. Щоправда ще в одному МЗС з'ясувалось, що лише 62,1% документації не підлягали будь-яким обмеженням у використанні, 26,7% призначалися для службового користування 9,4% – були конфіденційними та 1,8% – таємними⁶.

Після завершення холодної війни з'явився такий термін, як *"менеджмент ризиків"*, уперше запропонований американською Об'єднаною комісією з питань безпеки – підрозділом, тимчасово сформованим на початку 90-х років під егідою Міністерства оборони США та ЦРУ для оцінки нової ситуації, що склалася після розпаду Радянського Союзу та соціалістичного табору. Ця концепція передбачає збалансоване вироблення необхідних заходів для захисту "чутливої" інформації з урахуванням існуючих на кожний момент небезпек, вразливих місць, наявних можливостей та коштів. Вона була створена на противагу старій політиці, яка мала на меті максимальне уникнення всіх можливих ризиків.

Концепція менеджменту ризиків, хоч і була розроблена насамперед для використання військовими та розвідувальними установами, повною мірою застосовується в інших урядових структурах, що працюють з секретною інформацією, в тому числі в МЗС та закордонних представництвах. З появою цієї концепції з'явилася потреба в нових інформаційних продуктах, які, з одного боку, дали б міністерству можливість отримання повної інформації і присутності в комп'ютерних мережах, а з іншого захистили б чутливу інформацію від небажаного втручання, тобто забезпечили належне використання закритої та відкритої інформації.

З березня 1994 р. у Великій Британії почалася реалізація урядової програми дій із захисту інформації на основі рекомендацій комісії, створеної за особистою вказівкою прем'єр-міністра. Вона передбачала цілу низку заходів, зокрема запровадження нової системи класифікації

документів будь-якого рівня. На жаль, нам не вдалося дізнатися, чи привело використання цієї нової системи до зменшення кількості документів з тим чи іншим ступенем таємності, проте достеменно відомо, що саме ця мета ставилася при впровадженні цієї системи. Її зміст полягає у визначенні більш чітких критеріїв надання грифів секретності. Цікаво, що, як і при запровадженні багатьох інших інновацій у системах МЗС одна з причин здійснення цих кроків полягала в прагненні заощадити бюджетні кошти, оскільки будь-який документ з грифом секретності потребує особливих умов пересилання і користування, внаслідок чого зростають витрати міністерства.

Вже згадана американська Об'єднана комісія з питань безпеки рекомендувала запровадити замість чинної системи з трьома рівнями секретності, які доповнюються 12 підкатегоріями нову систему, яка поділяє класифіковану документацію на два рівні секретності.

Отже, інформаційна революція спонукає міністерства закордонних справ цілої низки країн Заходу шукати нові підходи у сфері захисту інформації. Поширюється визнання того, що міркування безпеки не повинні надто обмежувати використання інформаційних систем, оскільки в них міститься значний потенціал для підвищення ефективності діяльності МЗС. Дозволимо собі стверджувати, що в Україні ці нові підходи поки не прищепилися і старе прагнення максимально уникнути будь-яких ризиків психологічно превалує.

На користь ретроспективних підходів, більшою мірою характерних для часів "холодної війни", ніж для сучасної епохи інформаційної революції, працює і стереотипне уявлення, що інформація, з якою має справу МЗС, здебільшого цілком таємна. Про те, що це навряд чи відповідає дійсності, говорять вищенаведені цифри щодо реальної кількості документів, які заслуговують грифів таємності, у користуванні дипломатичної служби США. Процитуємо витяги з висновків спеціальної комісії, яка аналізувала зазначену проблему в США в 1984-1985 рр.: "...Очевидно, що обсяг секретних документів непомірно зріс. Безперечно, міністерство оборони потребує інформаційного захисту багатьох справ, якими йому доводиться займатися. Проте величезна кількість документів отримує грифи таємності невиправдано, як невиправданий і вибір грифів, які їм надаються. ...І хоча ніхто не забороняє перешкоджати зловживанням у цій сфері, мало хто має час для суперечок із тими, хто ці зловживання вчиняє"⁷.

Варто принаймні розглянути можливість використання концепції "менеджменту ризиків" у сфері захисту інформації в нашій державі, враховуючи при цьому і необхідність створення сприятливих умов розвитку комп'ютерних мереж в державних установах, насамперед в МЗС, присутність якого в Інтернеті має стати обличчям України в глобальних інформаційних системах.

Принагідно додамо, що, за нашою оцінкою, в Німеччині режим безпеки є більш ліберальним, ніж у країнах колишнього СРСР. Наприклад, в МЗС ФРН може увійти та вільно пересуватися будь-який власник дипломатичної акредитаційної картки. 29 січня 2000 р. в міністерстві вперше був проведений день відкритих дверей, коли будь-який бажаючий міг відвідати міністерство оглянути всі приміщення, в тому числі особистий кабінет міністра і навіть спостерігати за його роботою. Протягом дня міністерство відвідали 25 тис. осіб. Ця акція була проведена, з метою подолання хибного уявлення про МЗС як абсолютно засекречену установу⁸.

Що стосується практичних факторів, які потребують уваги при використанні сучасних інформаційних технологій у державних установах, наприклад при створенні комп'ютерної мережі в міністерстві закордонних справ, то західні експерти виділяють такі ключові моменти.

Використання інформаційних технологій не повинно бути питанням лише технічного персоналу. Рекомендується від самого початку призначити відповідальну особу з керівної ланки установи, яка б координувала та керувала діяльністю технічного персоналу.

Міністерству, як правило, потрібні не найсучасніші інформаційні технології, а системи, що працюють надійно й ефективно. Іншими словами, слід по можливості користуватись випробуваним програмним та апаратним забезпеченням.

При запровадженні нових інформаційних технологій варто мати на увазі, що жодна сфера не розвивається так швидко, як комп'ютерна галузь. Тому *треба завчасно потурбуватися, щоб жоден крок не блокував шляхи для подальшого розвитку.*

Користувачі нових технологій, скажімо, дипломати, які працюватимуть у єдиній мережі, повинні брати участь у формуванні концепції запровадження сучасних систем.

На всіх комп'ютерах у мережі має стояти ідентичний набір програмного забезпечення. Досвід МЗС ФРН також свідчить, що коли цей набір мало відрізняється від поширених програм, установлених на домашніх персональних комп'ютерах, це сприяє швидшій адаптації персоналу до роботи в мережі.

Слід заздалегідь передбачити регулярну ревізію апаратного і програмного забезпечення. В міру його застаріння воно має замінитись на сучасне.

Створювати нові комунікаційні системи слід "із запасом", тобто необхідно виходити з того, що інформаційні потреби з часом досить швидко зростають.

Важливими і поки мало дослідженими є соціальні та структурні аспекти запровадження нових інформаційних технологій в МЗС та інших державних установах. У більшості західних міністерств закордонних справ широке запровадження інформаційних технологій уже

привело до фактичного злиття підрозділів, відповідальних за зв'язок із закордонними місіями, та підрозділів, відповідальних за комп'ютерне забезпечення. Наприклад, Міністерство закордонних справ та торгівлі Канади здійснило програму перекваліфікації співробітників свого управління комунікацій ("*communications branch*") на "менеджерів інформаційних систем".

Нові інформаційні системи досить суттєво змінили способи, виконання міністерством його політичних завдань. Досвід роботи багатьох урядових структур на Заході показує, що нові технології можуть спричинити неочікувані зміни в їхній організаційній структурі. Більше того, дослідники цієї теми певний час дотримувалися думки, що "організація урядових установ у майбутньому буде напряму прив'язуватися до їх комп'ютерних мереж"⁹.

Інші фахівці звертають увагу на *подвійний вплив інформаційних технологій на роботу урядових установ. Вони можуть надати їй більш рутинного, механічного характеру або, навпаки, розширити свободу діяльності, поле компетенції державних службовців – користувачів комп'ютерних мереж; з одного боку їх можна використати для посилення ієрархічного контролю, а з іншого – для заохочення власної ініціативи співробітників та підвищення їхньої кваліфікації*¹⁰.

Зазначені дилеми незабаром постануть і перед керівниками міністерств та відомств в Україні. У цьому контексті цікавим є досвід приватних фірм на Заході, де запровадження комп'ютерних мереж привело до спрощення ієрархічних структур. Нерідко наслідком було скасування низки керівних посад середньої ланки, зростання відповідальності окремих співробітників, гнучкості в розподілі праці тощо.

На початку 90-х років прогнозувалося, що великий бізнес початку XXI ст. буде складатися з окремих груп, "команд" фахівців, підпорядкованих безпосередньо керівництву фірми, без середньої ланки менеджменту. "Ці підприємства більше нагадуватимуть за своєю структурою симфонічні оркестри", – писав П.Ф.Дракер у своєму дослідженні "Прихід нових організаційних структур" (1988)¹¹. Досвід сучасних фірм принаймні тих, які працюють у сфері розробки програмного забезпечення в комп'ютерній галузі, демонструє, що цей прогноз виправдовується.

Вже в 2000 р. журнал "Бізнес уік" написав, що в XX столітті основною формою організації праці була піраміда, а в XXI столітті нею стане віртуальна мережа.

Інформаційна революція провела нині чітку лінію між традиційними методами організації праці та інноваційними схемами. Більшість нових швидко зростаючих фірм, насамперед у галузі інформаційних технологій, віддають перевагу горизонтальним ієрархіям та мобільному менеджменту. За словами члена правління німецького

енергетичного концерну RWE Д. Швеєра, "коли всі письмові столи об'єднані в одну мережу, керівні ланки втрачають свої традиційні функції"¹². Під тиском двох основних чинників – зростаючої конкуренції та розвитку інформаційних технологій – великі концерни Заходу змушені шукати нових шляхів організації праці. Як наслідок сильні, гнучкі команди витісняють громіздкі вертикальні комунікаційні структури. Навколо сучасного менеджера виникають, працюють, зникають і знову виникають команди експертів, метою яких є якомога скоріше розв'язання поставлених конкретних питань за якомога оптимальнішого використання ресурсів. Це передбачає необхідність пошуку нових форм оцінки праці, винагороди співробітників та планування їх кар'єрного просування. Адже робота в команді та кар'єрне просування – це два елементи, оптимальне поєднання яких ще не знайдене.

Аналіз першого десятиріччя активного застосування новітніх інформаційних технологій у дипломатичних службах Заходу дає підстави для таких загальних висновків.

Інформаційна революція призвела до кардинальних змін у роботі дипломатичних відомств Заходу в 90-х роках, і динаміка цього процесу ще далеко не вичерпана. Комп'ютеризація міністерств та закордонних місій, їх об'єднання в спільній мережі, широке використання Інтернету та інших засобів комунікації спричиняють докорінні зміни в діяльності дипломатичних служб, приводять до їх більшої відкритості та мобільності.

Основними чинниками, які спонукають МЗС іти на такі зміни, є зростаюча роль інформаційних технологій, як інструменту політичного впливу, прагнення використати нові можливості ІТ для виконання дипломатією її повсякденних завдань, включаючи координаційну діяльність, захист економічних інтересів, зв'язки з громадськістю, консульські питання тощо. Додатковими спонукальними факторами тут є заощадження бюджетних коштів та використання потенціалу молодого покоління дипломатів, змалу знайомих з комп'ютерною технікою.

Широке використання ІТ дає можливість вивести на новий рівень і повністю перекласти на плечі техніки виконання суто механічних завдань контролю за діяльністю МЗС та закордонних відомств й оцінки їх фінансової ефективності. Для цього сучасні МЗС застосовують випробувані в приватному бізнесі програми контролінгу.

Повсюдне використання новітніх ІТ підвищує вразливість МЗС та закордонних відомств із погляду зору вимог безпеки, проте міністерства свідомо йдуть на цей ризик, зважаючи на багаті можливості, що відкриваються завдяки новим інформаційним технологіям. Як наслідок, на зміну традиційній секретності діяльності МЗС і нама-

ганням максимально виключити всі небезпеки приходить концепція менеджменту ризиків – всебічного зваження можливих небезпек та способів запобігання їм у кожному конкретному випадку.

Широке застосування інформаційних технологій може привести в МЗС до ефекту, що спостерігається у практиці приватного бізнесу, де комп'ютеризація нерідко спричиняє падіння або спрощення вертикальних ієрархій організації праці, звуження середньої керівної ланки, виникнення мобільних малих робочих груп або так званих команд, які створюються для вирішення конкретних, відносно вузьких завдань. Деякі організаційні зміни, що відбулися в МЗС країн Заходу останніми роками, свідчать про виникнення такої тенденції і в дипломатичній службі.

ПОСИЛАННЯ.

- ¹ Cash J. Corporate Information Systems Management. Irwin; 1992. – P.42-45.
- ² У 1992 р. на запровадження нових інформаційних технологій у Форін Офісі на десятирічний термін було виділено 32,5 млн. фунтів. Порівняно з грошима, що витрачаються на такі цілі, наприклад, великими банками, йдеться про досить помірну суму.
- ³ У МЗС ФРН така практика ще не налагоджена.
- ⁴ Найпоширенішою практикою, зокрема в міністерствах закордонних справ США та Великої Британії, є підключення до Інтернету окремих персональних комп'ютерів чи відокремлених мереж, завдяки чому міністерство отримує інформацію зовні, не відкриваючи свої власні системи для сторонніх користувачів. Те ж саме стосується закордонних місій.
- ⁵ Reinventing Government: Change at State. – Washington, 1993. – P.63.
- ⁶ Eldon S, "From Quill Pen to Satellite", Foreign Ministries in the Information Age. – London, 1996. – P.10.
- ⁷ Помар Н., Аллен Т.Б. Энциклопедия шпионажа. – М., 1999. – С. 564.
- ⁸ Volkswandierung im Außenamt/Suddeutsche Zeitung. – 2000. – 31.01.
- ⁹ Haigh R. Communications in the 21st Century. – New York, 1981. – P. 139.
- ¹⁰ Waltom E. Up und Running: Integrating It and the Organization. – Cambridge, Mass., 1989.
- ¹¹ Drucker P. The Coming of the new Organization // Harvard Business Review. 1988. Januar-February. – P. 45-53.
- ¹² Bissinger M., Kundt D., Schweer D, Konsens oder Konflikt? – Amburg, 1999. – P.169.