Інформаційні ризики в державному управлінні

Олександр СОСНІН,
професор кафедри управління суспільним розвитком Національної академії державного управління при Президентові України, доктор політичних наук, професор

Сергій ЯРЕМЕНКО,
аспірант кафедри управління суспільним розвитком Національної академії державного управління при Президентові України

Однією з основних ознак сучасного суспільного розвитку є функціонування інформації як стратегічного ресурсу в організаційній структурі державного управління, а тому особливого значення набуває надійність апаратури, алгоритмів і каналів передачі та поширення змістовної інформації. За допомогою сучасних засобів комунікацій вона активно переходить у загальнодоступну форму – інформаційний ресурс (ІР) державних установ в електронному вигляді.

Зумовлюючи стрімкий рух від індивідуального знання до знання соціуму, ІР у державних установах трансформується в електронні бази змістовної інформації, накопичуючись на серверах, доступ до яких часто є відкритим, зокрема, для транснаціональних компаній, численних структур провідних країн світу. Вони, маючи певний потенціал, підтримують за рахунок цих ресурсів власну економічну чи політичну спроможність.

Актуальність розробки проблематики створення, збереження і захисту ІР як окремого напряму в науці про державне управління зумовлена тим, що державна інформаційна політика, її формування й реалізація нині виходять на передній план загальної політики держави.

Стимулюючи розвиток і вимагаючи широкого впровадження нових засобів контролю за комунікаціями, які необхідні під час обміну інформацією чи навіть простого спілкування [1], слід пришвидшувати зміну правил, норм і законів щодо використання інформації в усіх сферах людської діяльності, підвищувати вимоги до процедур доступу до інформації, яку мають органи влади.

Багато злочинів пов'язані з використанням комп'ютерних систем, і їх кількість та різноманіття мають тенденцію до зростання. Наприклад, значного поширення набуло шахрайство з пластиковими картками банків (оплата товарів і послуг чужим коштом), із персональною інформацією громадян під час зміни платіжних документів тощо. За повідомленнями ЗМІ, в Росії протягом 2010 року в такий спосіб украдено близько 1 трильйона рублів. Системно розкрадаються масиви інформації банків, податкових служб, силових відомств, міліції – передусім із метою комерційного використання приватними особами.

Зрозуміло, що більшість таких тенденцій спричинена браком системного бачення процесів активного входження приватних структур у ринок облаштування сучасними засобами, зокрема й технологіями ІКТ (інформаційно-комунікаційні технології), органів державного управління. Це, безперечно, постійно розширює знання й уявлення про можливості ІКТ, однак експерти з безпеки звертають увагу на певну комерціалізацію ринку товарів та послуг у сфері державних замовлень, закидають навіть наявність тут контрольованого ринку. Його «учасники» прагнуть постійно розширювати свій бізнес, використовуючи різноманітні, часто непрозорі, схеми.

Відомо, що ІКТ у глобальному інформаційному просторі використовують досить широко, наприклад, для дестабілізації політичної ситуації й завдавання економічних збитків окремим регіонам світу, країнам, населеним пунктам, підприємствам і організаціям, а також громадянам. Тож під інформаційною безпекою держави розуміють цілковиту захищеність її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства й держави. Виокремлюють чотири основні складові інтересів України: **перша** – це «додержання конституційних прав і свобод людини і громадянина у сфері одержання

інформації і користування нею, забезпечення духовного оновлення України, збереження й укріплення моральних цінностей суспільства, традицій патріотизму й гуманізму, культурного й наукового потенціалу» країни; **друга** – інформаційне забезпечення державної політики України; **третя** – розвиток сучасних інформаційних технологій; **четверта** – захист інформаційних інтересів.

Цілком логічно постає наукове й практичне завдання – розкрити закономірності, умови, чинники й механізми сприйняття, засвоєння, переосмислення людьми інформації й побудови ними власної диспозиції. Звідси беруть витоки проблеми інформаційної безпеки. Основними критеріями державного управління в сучасних умовах тут, на наш погляд, стають:

– відповідність системи інформаційної безпеки сучасним викликам і загрозам;

– формування інформаційної культури громадян;

– створення умов для інформаційної рівності;

– наявність якісних джерел інформації;

– збереження цілісності соціальних комунікацій шляхом блокування неправомірних дій деструктивних сил;

– широка участь громадян у формуванні національного інформаційного простору та інформаційного законодавства, а також у вирішенні питання регулювання доступу до інформації.

Безперечно, використання навіть найдосконаліших методів контролю сучасних ІКТ в управлінні не гарантує абсолютної безпеки. Водночас мережі державного управління не можуть наражатися на непрогнозовані, навіть незначні ризики. Оцінювання цих ризиків є нетривіальним завданням, а необхідність передбачити їх під час проектування систем завжди є нагальною. До того ж через складність процесів адаптації людини до інформаційно-комунікаційного середовища слід вибудовувати принципово нові методи обробки інформації.

Зростання обсягів інформації призводить до виникнення проблем, усунення яких пов'язане з потребою глибоких теоретичних знань у різних наукових сферах. **По-перше**, відбувається накопичення неякісної інформації, яка вводить в оману користувачів або спотворює процеси набуття нових знань. **По-друге**, важлива інформація часто безпідставно утаємничується, внаслідок чого стає недоступною для аналізу її фахівцями. **По-третє**, великий обсяг інформації складно обробляти [2].

Згадані чинники негативно відбиваються на суспільстві, оскільки боротьба за інформацію завжди супроводжувалася боротьбою за владу, за можливість управляти справами суспільства, визначати напрями суспільного розвитку та використовувати фінансові й інші ресурси. Сфера соціально-політичного життя суспільства створювалася всією сукупністю суспільних відносин навколо знань та інформації, включаючи формування політичних документів, ідеологію, інформаційну економіку тощо.

І зазвичай на стадії їх практичного застосування між людьми й народами виникають певні непорозуміння і кордони, які суспільство змушене долати.

Створення, модернізація й підтримка працездатності комп'ютерних мереж є одним із недостатньо розроблених напрямів нашої науки й техніки. Наслідки неуваги до цієї сфери почали гостро відчуватися порівняно недавно. Проте свого часу, в епоху панування великих ЕОМ, державі вдалося створити інфраструктуру, здатну забезпечити будь-який рівень працездатності (доступності) всіх інформаційних систем протягом їх життєвого циклу. Інфраструктура містила як технічні, так і процедурні регулятори (навчання персоналу й користувачів, проведення робіт відповідно до апробованих регламентів тощо). Під час переходу до персональних комп'ютерів і технологій типу «клієнт–сервер» інфраструктура забезпечення доступу до ІКТ та інформації виявилася недосконалою, тому важливість розв'язання цієї проблеми істотно збільшилася. Наразі перед державними й комерційними організаціями гостро стоїть питання впорядкованості й регламентованості дій, властивих періоду панування великих ЕОМ, поєднання їх із технологічними можливостями, відкритістю й гнучкістю сучасних систем.

Потребує розв'язання ще одна загальнодержавна проблема – встановлення єдиного порядку реагування на порушення інформаційної безпеки. Припустімо, користувач або системний адміністратор зрозумів, що сталося порушення. Що він мусить робити? Поки що жодне відомство не запропонувало регламенту дій у таких екстремальних ситуаціях. За цих умов цілком очевидною є необхідність організувати національний центр інформаційної безпеки, до компетенції якого належали б, зокрема, інформування користувачів усіх рівнів про виникнення нових загроз і рекомендація заходів протидії, оперативна допомога організаціям у разі небезпеки.

Відомо, що масштаби комп'ютерної злочинності збільшуються (за винятком спаму) через ускладнення технологічних регламентів упровадження, модернізації та експлуатації апаратури. Додаючи до технологій управління величезну й складну сукупність нових знань, часто втаємничених, покажемо комплекс проблем на інтелект-карті (*див. рис. на стор. 26*).

Нові виклики й загрози державному управлінню пов'язані з розвитком глобальних інформаційних мереж, які передбачають постійне вдосконалення всіх елементів системи інформаційної безпеки. На нашу думку, є необхідним проведення широкомасштабних експериментів заради оцінки досягнутих інформатизацією країни результатів упровадження й експлуатації ІКТ у державних установах. Помилки, які буде виявлено, спонукатимуть до глибшого аналізу їхніх витоків і водночас до подальшої роботи з мінімізації загроз у державному управлінні.

Системне виявлення негативних тенденцій змушуватиме владу активізуватися, залучати до боротьби зі злочинністю в інформаційній сфері структури громадянського суспільства. Тоді виникне довіра до персоналу – творчих і освічених людей. А це стимулюватиме освітньо-виховні процеси в державі, заохочуватиме до заходів із підвищення кваліфікації працівників державних установ.

Діяльність із підтримання інформаційної безпеки відповідно до сучасних вимог є багатоплановою. Вона передбачає таке:

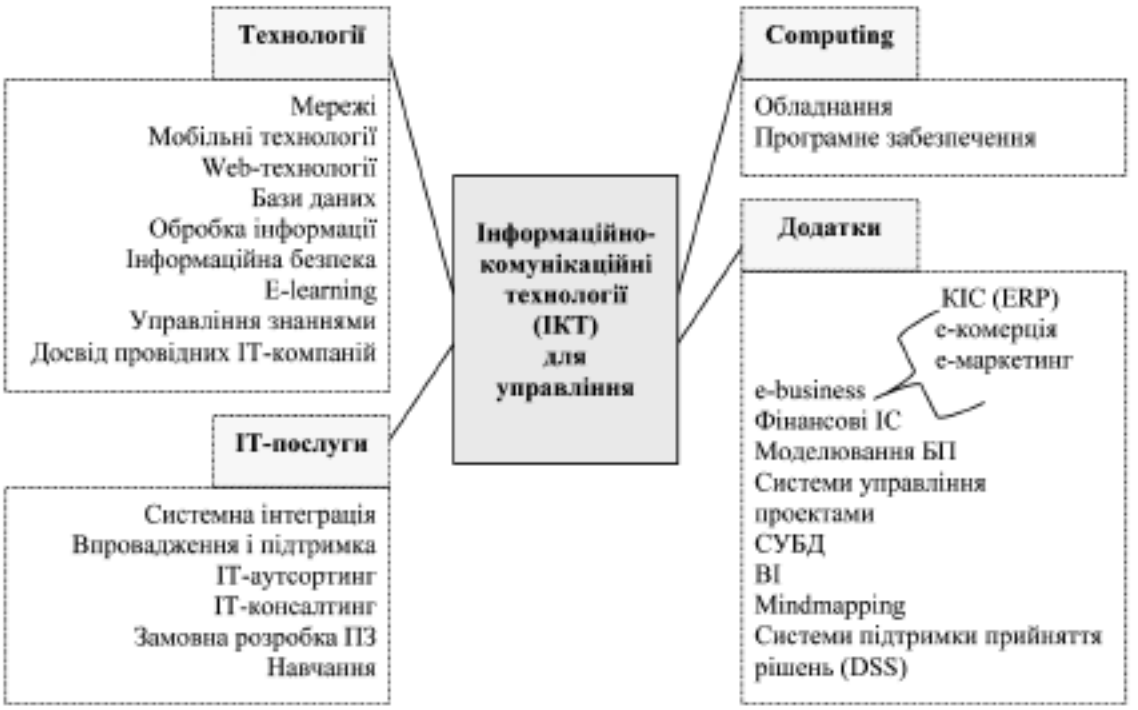
1. Проведення постійного моніторингу загроз інформаційної безпеки. У процесі моніторингу важливо встановлювати стадії розвитку небезпечних ситуацій і вчасно визначати першорядні загрози – це дасть змогу заощаджувати фінансові й матеріальні ресурси, підвищувати ефективність функціонування системи інформаційної безпеки.

2. Удосконалення законодавчої, нормативно-методичної й технологічної бази забезпечення інформаційної безпеки міста та його мешканців.

3. Налагодження стійкого партнерства з недержавними структурами міста у розв'язанні складних проблем гарантування інформаційної безпеки.

4. Створення штатного органу для забезпечення концептуального й координуючого складника роботи з інформаційної безпеки.

Отже, хоча сучасні інформаційно-комунікаційні технології стають ефективним інструментом підвищення рівня відкритості й доступності влади, важливим чинником збереження соціальної стабільності, економічного зростання й безпеки громадян, вивчати глобальний характер використання інформаційних технологій потрібно комплексно, тому що сучасні виклики диктують не-



Інтелект-карта ІКТ для державного управління

обхідність постійного вдосконалення систем безпеки, скоординованих дій державних органів і осередків громадянського суспільства.

Стрімке розкриття можливостей комп'ютерних технологій значно підвищило темпи системного акумулювання знань, їх узагальнення й оформлення як інформаційного ресурсу – особистого, суспільного, державного. Останнім часом ІР формується як окрема нематеріальна субстанція життєдіяльності суспільства в інформаційній сфері, «перетинання» якої набуває глобального виміру, перетворюючи знання та змістовну інформацію на ресурс інноваційного економічного й політичного розвитку планети.

Спроби унаявити процес руху індивідуального знання до колективного мають не тільки пізнавальне значення. Алгоритм тут дає змогу наочно встановити, так би мовити, вузлові пункти переходу інформації з одного стану в інший. Тоді можна зафіксувати зону правового регулювання відносин і поводження суб'єктів на певному етапі роботи й контакту з інформацією, продуктами інтелектуальної власності, суміжними правами. Саме цей непростий механізм забезпечить виявлення об'єктивно зумовлених предметів нормативного (правового, технічного й іншого) регулювання в інформаційній сфері.

Набуваючи властивостей популярного товару, інформаційні ресурси за допомогою інформаційно-комунікаційних технологій об'єднують основні сектори економіки та політики. Вони активно переміщуються у світовому віртуальному інформаційному просторі, збільшуючи залежність суспільства, окремих сфер його життєдіяльності від загальносвітових процесів виробництва, накопичення, поширення й використання інформації, перетворюють її на об'єкт різноманітних економічних і суспільних відносин, що, своєю чергою, стимулює швидкий розвиток технологій, створення електронних масивів інформації, які стануть складовою інформаційних ресурсів світу.

Скажімо, процеси електронізації інформаційних ресурсів дадуть змогу не тільки трансформувати їх в електронну форму, а й підвищити питому вагу інтелектуальних моделей. Сучасні технології зберігання електронних ресурсів забезпечують оперативне управління інформацією, що зберігається в інформаційних сховищах, позаяк в основу створення електронних ресурсів покладена концепція статичних і динамічних документів. Тут кожний тип документів, що містять інформацію про конкретні факти, унаявлюється у вигляді набору віртуальних моделей з власними характеристиками й атрибутами. Їх еволюція, безумовно, завершується цілковитою електронізацією інформаційних ресурсів у бізнесі, освіті й управлінні. Системні дії щодо електронізації інформаційних ресурсів стають підґрунтям для розвитку новітніх технологій промислового виробництва й державного управління.

Погодьмося, що робота будь-якої інформаційно-комунікаційної системи впливає на інші. Взаємні контакти фіксуються, розширюючи простір для глибокого й різнобічного аналізу обсягів інформації, що постійно зростають. Це породжує проблему захисту інформації від витоку технічними каналами для потреб нових, іноді віртуальних, користувачів інформаційних ресурсів організацій і установ. Водночас розробляються технічні засоби, що накопичують, аналізують потоки інформації, підвищують ризики несанкціонованого відбору службової інформації.

З огляду на те, що людина стала медіа-активним компонентом ІКТ, корупція з'явилася у сфері новітніх інформаційно-правових відносин, порушивши засади юридичної науки, яка традиційно визначала це явище лише як зловживання владою. Тож до вивчення проблем корупції долучилося широке коло фахівців із суспільно-політичних наук, які стали ширше трактувати її зміст. Так, до поняття корупція тепер входить і отримання переваг від володіння і використання втаємниче-

ної законом інсайдерської інформації. Це виявляється під час аналізу проектів розвитку суспільства, патентів, наукових статей і дисертацій для високопосадовців, а наслідком має створення сімейних кланів у політиці, державному управлінні, науці, дипломатії тощо. Наприклад, порушуючи традиції конфіденційності інформаційного обміну, чиновники забезпечують доступ своїм висуванцям до інсайдерської інформації, аби ті мали переваги під час отримання посад, пов'язаних із розподілом державних ресурсів.

Трансформація ризиків зумовлюється, зокрема, прискоренням інтеграційних процесів – економічних, технологічних, культурних тощо. Це посилює ризикованість і венчурність під час обміну інформацією. Задовольняючи потреби в ефективності управління, новітні ІКТ породжують технологічні проблеми, що негативно впливають на сталий розвиток суспільно-політичного середовища країни.

Джерела

1. *Д. Гринберг, Р. Байрон.* Организационное поведение: от теории к практике. – М.: Вершина, 2004.

2. *Негодаев И. А.* На путях к информационному обществу. – Ростов-на Дону: Изд-во Донского гос. техн. ун-та, 1999. [Электронный ресурс]. – http:lib.socio.msu.ru /1/library?e=d-001ucheb-00-0-0-0prompt-10-1251-00&a =d&cl=CL.2.83

До питання про концептуальні підходи у реформуванні системи адміністративно-територіального устрою в Україні

Людмила ТВАРКОВСЬКА,
ад'юнкт Національної академії внутрішніх справ

Серед науковців зазначену проблематику частково досліджували Р. Безсмертний, А. Доценко, В. Кравченко, І. Кресіна, А. Коваленко, В. Олуйко, С. Телешун та інші.
За участю науковців напрацьовано низку концепцій адміністративно-територіальної реформи (АТР) та вдосконалення системи територіальної організації влади в Україні, зокрема: проект концепції реформи місцевого самоврядування, Концепція реформи адміністративно-територіального устрою (АТУ) України, яка визначає основні засади організації АТУ та формування адміністративно-територіальних утворень, їхню типологію; організацію публічної влади на відповідних рівнях; законодавче забезпечення та етапи проведення адміністративно-територіальної реформи. Водночас зазначених концепцій досі не реалізовано, що свідчить про недостатнє наукове обґрунтування їх та не дає можливості усунути недоліки в системі АТУ України.

Окрім того, деякі розробки з удосконалення нормативної бази законодавства АТУ здійснено Асоціацією міст України. Зокрема, розроблено проект закону України «Про порядок вирішення питань адміністративно-територіального устрою України», який визначає поняття та засади АТУ України, правовий статус і рівні адміністративно-територіальних одиниць (АТО) та ін. Ст. 4 проекту закону України «Про основні засади розвитку місцевого самоврядування в Україні» визначає, що одним із головних завдань державної політики з розвитку місцевого самоврядування є зміна системи АТУ України з метою формування територіальної основи місцевого самоврядування [12]. Також розроблено проект закону України «Про адміністративно-територіальний устрій України». Документ визначає поняття, засади й систему АТУ України, рівні АТО, порядок вирішення органами державної влади та органами місцевого самоврядування питань АТУ. Процес законодавчої підготовки законопроекту все ще триває, й відповідно потребує подальших наукових досліджень.