Ягодзінський Сергій Миколайович
д-р філос. наук, професор
Національний авіаційний університет,
м. Київ, Україна

КУЛЬТУРА БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційне суспільство висуває до людини низку вимог технологічного характеру. Володіти системним мисленням, використовувати інноваційні технології, мати високий рівень технічної грамотності стало не лише потребою, а й частиною культури безпеки суспільства, що входить у стадію четвертої індустріальної революції. На початку XXI ст. формується нова модель реалізації інформаційних взаємодій, основу якої складає система глобалізованих інформаційних мереж. Якщо наприкінці минулого століття інформаційні канали слугували для трансляції інформації між органами влади, спеціальними службами чи міжвідомчими структурами, то нині доступ до інформаційних баз є умовою соціально-економічного розвитку. Постіндустріальне суспільство стало першим в історії, в якому інноваційна діяльність перетворилася на норму. Найбільш виразно це продемонстрував А. Норман, який називає економіку інформаційного суспільства економікою відкриття, винаходу та інновації [1]. Історичні етапи, в його інтерпретації, вже не вимірюються науково-технічними революціями. Останні у формі технологічних новацій (нерідко дизруптивних – підривних) перетворилися на буденність. Стає очевидним, що в умовах інформаційного суспільства існувати – означає бути присутнім у глобальному інформаційному середовищі. З часу ж виникнення інформаційних мереж мета, способи й засоби такого представлення перманентно еволюціонували. Ключову роль у цьому процесі відігравали соціальні мережеві сервіси, які функціонують у форматі Web 2.0. Зазначені технологічні можливості розкривають інноваційний потенціал техніко-економічного, політико-правового і культурно-історичного вимірів суспільного прогресу та детермінують його темп.

Поява інформаційних мереж, з одного боку, сприяла пришвидшенню глобалізаційних процесів, а з другого – призвела до диференціації світового співтовариства залежно від доступу до наповнення і користування інформаційними ресурсами. В умовах, коли інформація, теоретичне знання і технології перетворилися на продуктивну силу соціально-економічного, наукового і технологічного розвитку, розвинена інфраструктура соціальних мережевих сервісів стала умовою національної й регіональ-

ної безпеки, інноваційної політики та промислової конкурентоспроможності. Виходячи з цього, фундаментальною проблемою сучасного соціально-філософського пізнання є розробка методології й методики оцінки інноваційного потенціалу, який можна реалізувати за посередництва мережевих сервісів, таких як блоги, сервіси cloud computing, економічні, політичні платформи, класифікатори баз даних, віртуальні наукові товариства, новітні форми надання освітніх послуг, Wiki-проекти, медійні бази даних, електронний документообіг тощо.

Побіжно це виражено в актуалізації проблеми розробки ефективних засобів захисту інформації. Для запобігання комп'ютерних злочинів розроблені й діють технічні, організаційні та правові заходи. До технічних відносяться: захист від несанкціонованого доступу до інформаційних систем; процедури резервування; диверсифікація обчислювальних мереж на випадок інформаційних нападів, саботажу, диверсій тощо. До організаційних заходів належать: охорона обчислювальних центрів; підбір персоналу; організація обслуговування обчислювального центру сторонніми особами (аутсорсинг); розвиток корпоративної культури співробітників; універсальність засобів захисту для користувачів. До правових заходів відносять: відповідальність за комп'ютерні злочини; захист авторських прав власників інформаційних ресурсів; удосконалення карного й цивільного законодавства; прийняття міжнародних договорів про права і обов'язки фізичних чи юридичних осіб, які обслуговують комп'ютерні мережі тощо. Але й такий розгалужений комплекс заходів не є повноцінним гарантом стабільності інформаційних систем. Несправності обладнання, неефективність алгоритмів обробки даних, некоректність роботи комунікативної складової інформаційних мереж, кібератаки, зношення устаткування, людський фактор при обслуговуванні складних систем – ці та інші фактори безпосередньо впливають на процеси забезпечення функціональності соціуму як складної самоорганізованої системи.

За таких умов питання надійності, безвідмовності апаратної та програмної складових реалізації інноваційних технологій постає як нетривіальна і перманентно актуальна проблема, оскільки вона стосується не лише забезпечення процесів життєдіяльності суспільства, а й безпеки кожної людини. Адже майже всі, хто використовував сучасні технологічні пристрої, зіштовхувалися із ситуаціями, які можна схарактеризувати наступними словами: «зависання», «перевантаження», «аварійне закриття», «неприпустима операція», «неадекватна реакція або її відсутність», «втрата чи псування даних» і т.п. Причиною таких збоїв є як помилки, допущені на етапах проектування і створення програмних кодів, так і не-

врахування архітекторами, програмістами та інженерами ситуацій, коли процеси, що не є зв'язаними безпосередньо, за певних умов вступають у конфлікт. Відомий письменник-фантаст, популяризатор науки А. Азімов у циклі розповідей «Я, робот» неодноразово підкреслював, що програмні помилки здатні накопичуватись, провокуючи появу незапланованих, неочікуваних реакцій.

Означене змушує закріпити за державою важливу функцію в розбудові інформаційного простору, а саме – реалізацію інформаційної безпеки соціальних агентів. Адже деструктивні інформаційні впливи у формі пропаганди, маніпуляції, дезінформації орієнтують органи влади не стільки на розвиток мережевої архітектоніки, скільки на її захист. Дослідники виокремлюють кілька аспектів інформаційної безпеки [2, с. 196]: захищеність інформаційних ресурсів; надійність функціонування інформаційно-комунікативних систем; протистояння негативним інформаційним впливам на суспільну й індивідуальну свідомість; готовність до інформаційного захисту (як на психічному, так і на технічному рівнях). І хоча в світі існує незначна кількість глобальних інформаційних мереж, відсутність яких реально могла б відчутно негативно вплинути на життєдіяльність та добробут соціуму, кожен відчуває дискомфорт без доступу до Інтернету, стільникового зв'язку, систем супутникової навігації тощо, які можуть стати об'єктами інформаційного нападу.

Тобто на даному етапі цивілізаційного розвитку держава має підстави втручатися в інформаційні відносини та інформаційні процеси, що відбуваються або проходять її територією. Цей висновок корелює з процесом становлення світових правових систем, в якому чітко визначені різновиди інформаційних відносин, що потребують соціокультурної оцінки та правового захисту. По-перше, це відносини, зв'язані з функціонуванням Інтернету і доступом до нього. По-друге, відносини у сфері електронної комерції стають домінантними, оскільки несуть користь як споживачу, так і виробнику. По-третє, відносини щодо захисту авторських та інших виключних прав на об'єкти інтелектуальної власності, які розміщені в інформаційному просторі. По-четверте, відносини, що виникають стосовно захисту конфіденційності інформації, запобігання розповсюдження інформації приватного змісту.

Дотримання цих умов має забезпечувати соціальну рівновагу як діапазон збереження стабільності світоглядних орієнтирів, значення яких залежить від наявного в соціумі порогу дій та статусу носіїв репутації. При цьому рівновага колективної поведінки, яка й є кінцевою метою впливу на соціальні процеси, може бути досягнута через контроль імо-

вірнісного показника готовності до дії агентів мережі. При рефлективному управлінні суб'єкт на основі симулякрів вимушений відтворювати прообраз соціальної реальності з деякими видозміненими її параметрами та забезпечувати зворотній зв'язок. Натомість вивести систему колективної поведінки зі стану рівноваги можна й через вплив на рівень порогів агентів мережі. За таким способом соціального управління у соціальних науках закріпився термін «інформаційна атака». Основною метою такого типу атак є формування у масовій свідомості стану соціальної ажитації.

Управління соціальними процесами у формі інформаційної атаки не потребує зворотного зв'язку між інформаційними мережами, оскільки воно здійснюється опосередковано у площині відповідальності агентів і стабільності комунікативних зв'язків між ними [3, с. 59]. Соціальна рівновага за таких обставин досягається завдяки вибірковості об'єктів впливу, переорієнтації матриці довіри та коригування стимулів дій мережевої спільноти. Аналізуючи масив наукових праць із проблем управління, ми не знайшли усталеної відповіді на запитання: як формується матриця довіри в соціальних мережах та як на її основі відбувається їхня контамінація? Але при цьому очевидно, що низький рівень культури безпеки в інформаційному просторі провокує появу ситуативних матриць довіри, які використовуються для маніпуляції, транслювання ідей, символів та ідеологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Norman A.C. Information Society: An Economic Theory of Discovery, Invention, and Innovation. – Boston: Kluwer Academic Publishers, 1993. – 342 p.
2. Ананьїн В.О., Пучков О.О. Інформаційна безпека як складова національної безпеки України // Гілея: науковий вісник. – 2014. – Вип. 85. – С. 195-198.
3. Казимир В.В., Серая А.А. Метод построения моделей информационных атак // Математичні машини і системи. – 2010. – № 4. – С. 52-61.