ФІЛОСОФІЯ

УДК 101:37

СОЦІАЛЬНО-ФІЛОСОФСЬКЕ ОСМИСЛЕННЯ ПОНЯТТЯ «ІНФОРМАЦІЙНА БЕЗПЕКА»

Є. О. Архипова
викладач кафедри філософії
Національного технічного університету України
«Київський політехнічний інститут»

У статті окреслено основні підходи до розуміння поняття інформаційної безпеки, проаналізовано деякі термінологічні та методологічні аспекти, які мають неоднозначне трактування у вітчизняних та зарубіжних джерелах. Проаналізовано деякі аспекти нормативно-правової бази у сфері інформаційної безпеки. Запропоновано авторське визначення інформаційної безпеки. Акцентовано увагу на нетотожності термінів «інформаційна безпека» та «безпека інформації», доведено, що остання виступає лише одним із складових елементів інформаційної безпеки. Розглянуто загрози безпеці інформації та загрози деструктивного інформаційного впливу на свідомість і буття людини та суспільства. З числа загроз безпеці інформації докладно проаналізовано інсайдерські загрози, які виникають у внутрішньому середовищі організації. Названі можливі наслідки деструктивного інформаційного впливу на свідомість людини.

Ключові слова: інформаційна безпека, деструктивний інформаційний вплив, безпека інформації.

Необхідною умовою формування глобального інформаційного суспільства є розвиток різноманітних засобів комунікації та зв'язку, новітніх інформаційних технологій, що дозволяють більш ефективно та з меншими часовими і матеріальними витратами здійснювати пошук, обробку, синтез, передачу інформації. Різновекторні інформаційні потоки пронизують практично усі сфери суспільного життя, тому від вміння їх створювати та використовувати багато в чому залежить успішність і результативність діяльності соціальних суб'єктів будь-якого структурного рівня.

Характерною особливістю інформаційного суспільства є зростання ролі інформації, яка стає умовою ефективної діяльності, стратегічним ресурсом розвитку і продуктом виробництва. З іншого боку, негативний інформаційний вплив здатний зашкодити суб'єкту інформаційних відносин: завдати фінансових або матеріальних збитків, призвести до дисфункції або, навіть, фізичної загибелі. Ці загрози належать до сфери інформаційної безпеки, яка в сучасних умовах набуває надзвичайної актуальності та потребує ґрунтовного соціально-філософського дослідження з метою узагальнення існуючих даних, моделей, підходів і синтезування інтегруючої основи, здатної протидіяти новим викликам соціуму.

На сьогодні з поняттям «інформаційна безпека», зокрема, з його термінологічним визначенням, склалася парадоксальна ситуація. З одного боку, термін «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та законодавчих документах різного рівня, з іншого боку, це поняття досі не має однозначного розуміння, а його зміст у різних джерелах має кардинальні розбіжності. Відсутність центральної дефініції у сфері інформаційної безпеки обумовлює методологічну невизначеність ряду інших положень та термінів, що приводить до полісемії і значно знижує ефективність та прикладне значення наукових розробок в області інформаційної безпеки. З'ясування сутності цього терміну і є метою даної статті.

Питання інформаційної безпеки в тому чи іншому ракурсі розглядаються такими вітчизняними і зарубіжними дослідниками як Г. Атаманов, В. Богуш, В. Лопатін, О. Додонов, Б. Кормич, О. Литвиненко, Г. Смолян, О. Соснін, О. Юдін. Проте аналіз наукової літератури показує, що теоретичні та філософсько-методологічні аспекти дослідження інформаційної безпеки розроблені недостатньо глибоко, а дисциплінарна розрізненість наявного знання знаходиться в незнятому протиріччі з комплексним характером задач безпеки.

Офіційне визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: «інформа-

ційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [*1*].

На жаль, поява цього визначення не зменшила кількості дискусій щодо поняття інформаційної безпеки, що яскраво ілюструє різноманіття його трактувань в профільних виданнях. Так у навчальному посібнику 2009 р. [*5*, 28] інформаційна безпека визначається значно вужче – як «стан захищеності інформації від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації». У книзі 2008 р. [*3*] читаємо: «Інформаційна безпека може розглядатися у широкому і вузькому розумінні. У вузькому – як безпека інформації, у широкому – це стан захищеності як від загроз безпеці інформації, так і від загроз нанесення шкоди інформаційним технологіям». У наукових статтях також наявна термінологічна плутанина (див., напр., [*4*]). Схожа ситуація із розумінням змісту інформаційної безпеки і в російських виданнях.

Чому ж така ключова категорія як інформаційна безпека досі не набула усталеного тлумачення, тим більше, що її вивчення здійснюється на досить високому професійному рівні з широким залученням зарубіжного досвіду, сконцентрованому, в тому числі, в міжнародних стандартах? Певною мірою це обумовлено тим, що проблематика інформаційної безпеки є дуже складною та багатоаспектною. Крім того, часто вітчизняні та російські дослідники запозичують основний зміст визначення терміну з міжнародних стандартів, не враховуючи те, що термін «information security» може перекладатись з англійської як «інформаційна безпека» так і «безпека інформації».

Досить часто ці терміни використовуються як синоніми. Якщо об'єктом захисту виступає власне інформація, то поняття «інформаційна безпека» і «безпека інформації» дійсно синонімічні. Але, якщо у якості об'єкту захисту розглядається деякий учасник інформаційних відносин, то слово «інформаційна» у терміні «інформаційна безпека» вказує на напрям діяльності, за допомогою якої може бути заподіяна шкода об'єкту захисту. У цьому випадку поняття «інформаційна безпека» варто трактувати як стан захищеності деякого об'єкту від загроз інформаційного характеру і його заміна на термін «безпека інформації» є помилковою. У даному разі інформаційна безпека є ширшим за обсягом поняттям і включає в себе безпеку інформації.

Проте переважна більшість авторів наукових статей та навчальної літератури, які у своїх роботах підіймають проблему інформаційної безпеки, ототожнюють її із безпекою інформації. Пояснюється це тим, що в Україні, як і в інших країнах пострадянського простору, основна увага громадськості сконцентрована винятково на проблемі захисту інформації. У першу чергу така ситуація обумовлена тим, що інформація в сучасному світі стала товаром, а товар потрібно захищати. По-друге, це пояснюється професійною підготовкою фахівців, що першими усвідомили гостроту проблеми, адже переважна більшість з них – це представники технічних спеціальностей. Велике значення має те, що вітчизняні та російські дослідники не враховують, що міжнародні стандарти, з яких запозичується визначення терміну *information security*, належать до сфери безпеки інформаційних технологій, де об'єктом захисту виступає саме інформація (а не людина, суспільство чи держава). Таке фрагментарне запозичення ключових термінів з іномовних джерел без урахування загального контексту документів призводить до суттєвої плутанини в термінологічних визначеннях.

Так, у стандарті BS ISO/IEC 17799 *Information security* характеризується забезпеченням конфіденційності, цілісності та доступності інформації, а в ISO/IEC 27001 – як «всі аспекти, пов'язані з визначенням, досягненням та підтримкою конфіденційності, цілісності, доступності, невідмовності, підзвітності, автентичності та достовірності інформації чи засобів її обробки». Ці визначення стосуються поняття «безпека інформації» і, до речі, більш-менш збігаються з вітчизняним нормативним визначенням, наведеним у «Концепції створення Єдиної державної автоматизованої паспортної системи», де безпека інформації розуміється як «захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводить до модифікації, розкриття чи руйнування даних». Хоча, на наш погляд, таке трактування безпеки інформації є дещо звуженим, оскільки не включає забезпечення доступності інформації.

З цієї точки зору найбільш вдалим визначенням ми вважаємо наступне: безпека інформації – це стан захищеності інформації від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації [*7*].

Після викладеного вище спробуємо інтерпретувати наведене вище поняття інформа-

ційної безпеки і дати його соціально-філософське визначення. Для цього перш за все проаналізуємо зміст словосполучення «стан захищеності». Воно виражає кількісну або якісну ознаку рівня захищеності кого-, чого-небудь. Так, для якісної оцінки можливі характеристики захищеності на зразок: мінімальна, задовільна, низька, достатня, абсолютна тощо. Стан захищеності – це змінна у часі величина, яка залежить від інтенсивності та значущості інформаційних загроз, а також дієвості та ефективності системи захисту.

Наступне словосполучення, яке слід прокоментувати, – це «життєво важливі інтереси людини, суспільства та держави». По-перше, рівень інформаційної безпеки здатний знижуватися і при порушенні інтересів, які не можна віднести до життєво важливих, тому таке формулювання є не зовсім коректним. По-друге, категорія «інтереси» погано піддається формалізації, є надто розмитою та суб'єктивною. Так, відповідно до усталених поглядів, інтереси суспільства в інформаційній сфері полягають «у зміцненні демократії», «у забезпеченні інтересів особистості в цій сфері», «створенні правової соціальної держави», «у духовному відновленні держави» тощо. Насиченість правового документа такими нормами-деклараціями означає фактичну відсутність будь-якої його регулятивної сили, що, в свою чергу, призводить до появи нормативно-правових актів, не забезпечених механізмами їх юридичної дії, створює прогалини в правовому регулюванні питань інформаційної безпеки. Тому нам видається доцільним підшукати заміну виразу «життєво важливі інтереси».

У статті 1 Закону України «Про основи національної безпеки України» поняття «національні інтереси» визначається як «життєво важливі матеріальні, інтелектуальні і духовні цінності українського народу..., визначальні потреби суспільства і держави...». В стандартах використовується поняття «активи», яке за своїм змістом наближене до поняття «важливі цінності». Зокрема, в ДСТУ ISO/IEC 13335-1 визначається: «активи організації – усе, що має цінність для організації». За аналогією, до активів (взагалі, а не лише організації) можна віднести все, що має цінність для особистості, суспільства, держави, причому через оцінку ушкодження активів можна визначити рівень сукупної шкоди, заподіяної внаслідок реалізації інформаційних загроз, чим і визначається рівень інформаційної безпеки об'єкту [*2*].

Таким чином, у визначенні інформаційної безпеки *захист життєво важливих інтересів* ми пропонуємо замінити *захистом існування, функціонування чи діяльності* деякого об'єкта, причому в даному випадку якість захисту має досить чіткі критерії визначення, що ґрунтуються на обрахунку можливої чи вже заподіяної шкоди.

Останнім елементом в інтерпретованому визначенні інформаційної безпеки є перелік можливих інформаційних загроз, які можна поділити на два класи: загрози, спрямовані безпосередньо на інформацію, інформаційні ресурси та складові інформаційної інфраструктури деякого об'єкту (для протидії цим загрозам створюється система захисту інформації, що має гарантувати *безпеку інформації* на об'єкті), та інформаційні загрози більш загального характеру, які впливають на елементи середовища та безпосередньо на суб'єкта інформаційних відносин.

Отже, враховуючи вищенаведені аргументи, можна сформулювати таке визначення: інформаційна безпека – це стан захищеності людини, суспільства та держави від інформаційних загроз, який визначається рівнем шкоди, що може бути заподіяна існуванню, функціонуванню чи діяльності цих об'єктів в разі а) використання неповної, несвоєчасної та невірогідної інформації; б) здійснення негативного інформаційного впливу; в) протиправного застосування інформаційних технологій; г) порушення цілісності, конфіденційності та доступності інформації.

У даному визначенні основний наголос робиться не на захисті життєво важливих інтересів (категорії достатньо аморфної і суб'єктивної через відсутність чіткого законодавчого визначення), а на забезпеченні (збереженні) умов, необхідних для нормального існування, життєдіяльності, функціонування об'єкту захисту, причому загальноприйняті вимоги щодо цих умов визначаються та регулюються низкою документів, зокрема Загальною декларацією прав людини, Конституцією України, Господарським кодексом України, Кодексом України про працю тощо.

Узагальнюючи наведене вище, пропонуємо наступне соціально-філософське визначення: інформаційна безпека – стан захищеності свідомості та буття соціальних суб'єктів від інформаційних загроз, який визначається рівнем реальної чи потенційної шкоди, заподіяної внаслідок деструктивного інформаційного впливу або порушення безпеки інформації.

Порушити безпеку інформації можна шляхом впливу на інформацію та інформаційну інфраструктуру об'єкту захисту: пошкодити чи викрасти інформацію, зруйнувати технічні засоби, вивести з ладу програмне забезпечення чи системи зв'язку, підкупити персонал. Крім загроз антропогенного характеру, інформація може постраждати від техногенних та стихійних загроз.

Основними властивостями інформації як об'єкту захисту є доступність, цілісність та

конфіденційність. Доступність інформації визначається як можливість використання інформації та даних тоді, коли в цьому виникає необхідність. Інформація стає недоступною у разі блокування чи знищення інформації та засобів її обробки. Цілісність інформації – це її захищеність від несанкціонованої зміни, забезпечення повноти і точності інформації та методів її обробки. Цілісності інформації загрожує її фальшування, несанкціонована модифікація, викривлення тощо. Конфіденційність – це властивість інформації не підлягати розголосу, яка забезпечується шляхом доступу до інформації тільки авторизованих користувачів. Загрози порушення конфіденційності спрямовані на розголошення інформації з обмеженим доступом. Безпека конфіденційної інформації, тобто інформації з обмеженим доступом, може бути порушена внаслідок її несанкціонованого копіювання, викрадення або втрати.

Усвідомлення важливості захисту інформації та інформаційних ресурсів від загроз зовнішнього характеру відбулося вже досить давно і можливості такого захисту дуже широкі. Натомість недостатньо уваги приділяється так званим інсайдерських загрозам, які мають внутрішню природу. Інсайдерські інциденти відбуваються значно частіше, ніж зовнішні атаки, хоча компанії, як правило, намагаються не афішувати свої внутрішні проблеми. За даними PricewaterhouseCoopers та CXO Media, які опитали більше 13 тис. компаній в 63 країнах світу, в тому числі в Росії та Україні, 60 % всіх інцидентів у 2005 р., пов'язаних з IT-безпекою, відбулося саме в результаті дій інсайдерів [*6*, 31].

Абсолютно всі аналітичні звіти вказують, що найбільш небезпечною інсайдерською загрозою є витік конфіденційної інформації. Так за результатами дослідження Національної служби США з управління інсайдерськими загрозами (National Survey on Managing the Insider Threats), середні щорічні збитки від витоку інформації із розрахунку на одну опитану компанію складають $ 3,4 млн. Для порівняння: аналогічний показник втрат внаслідок вірусних атак за даними CSI/FBI Computer Crime and Security склав менше $ 70 тис.

Джерелом потенційних загроз в середині організації є невдоволені, ображені та корисливі працівники. Витік інформації може відбутися і без злого умислу: внаслідок необережності, халатності або застосування до лояльно налаштованих працівників організації методів соціального інжинірингу, під яким розуміється маніпулювання людиною або групою людей з метою зламу систем безпеки та викрадення важливої інформації. Соціальна інженерія може вважатися різновидом соціального програмування, але використовується лише в негативних цілях та лише по відношенню до людей, які є частиною комп'ютерної системи або мають доступ до секретної інформації.

Найбільші збитки через дій інсайдерів у 2006 р. за даними російської бази інсайдерських інцидентів InfoWatch було нанесено гіганту військової індустрії Lockheed Martin та Міністерству у справах ветеранів США. Три інсайдери з корпорації Lockheed Martin передали конкурентам результати проекту по розробці тренувальної системи для пілотів ВПС США та план дій компанії в боротьбі за контракт Пентагону вартістю $ 1 млрд. Вся інтелектуальна власність витекла з Lockheed Martin через банальні USB-флешки та CD/DVD-приводи.

У наступному місяці ненавмисним інсайдером став співробітник Міністерства у справах ветеранів США, який забрав додому ноутбук з персональними даними 26,5 млн. колишніх військових. На ліквідацію наслідків витоку інформації, що стався внаслідок пограбування домівки та викрадення ноутбуку, було виділено $ 500 млн. Крім того кошти пішли на організацію гарячої лінії, розсилку поштових повідомлень, надання потерпілим безкоштовної послуги по моніторингу кредитної активності та компенсаційні виплати. Потенційний збиток від витоку інформації становив $ 26,5 млрд. [*6*, 34].

Отже, за різними оцінками від 60% до 80 % збитків від витоку, втрати чи несанкціонованого доступу до інформації виникають через дії осіб всередині організації. Тому при осмисленні феномену інформаційної безпеки обов'язково потрібно враховувати цей вид загроз.

Звернемося тепер до другої складової інформаційної безпеки – захисту свідомості та буття соціальних суб'єктів від деструктивних інформаційних впливів. Зауважимо, що сучасна рефлексія інформаційної безпеки є досить однобічною: питання безпеки інформації, зокрема розробки систем захисту, характеризуються достатньо високим рівнем теоретичного та практичного розвитку, натомість проблематика деструктивних інформаційних впливів розроблена значно гірше і представлена в основному описами окремих ситуацій та сценаріїв, або у вигляді вельми абстрагованої теорії.

Взагалі чіткі межі негативних інформаційних впливів ще не окреслені, тому до них відносять широке коло явищ: від соціальної інженерії до PR-елементів рейдерських операцій. Крім безпосереднього впливу на інформацію та інформаційну інфраструктуру об'єкту захисту, загрозу становлять зовнішні по відношенню до об'єкту захисту інформаційні впливи: наприклад наклеп та обмова, які реалізуються

через чутки і засоби масової інформації. При цьому дані, що циркулюють в інформаційній системі організації зберігають абсолютну недоторканість, а традиційні загрози цілісності, доступності, конфіденційності та іншим властивостям інформації відсутні.

Крім того, слід зазначити, що негативним інформаційним впливом може бути оприлюднення навіть правдивої інформації. Так, якщо фірма використовує технології, що забруднюють оточуюче середовище, то оприлюднення цього призведе до погіршення її іміджу і, можливо, інших втрат, в тому числі фінансових, хоча, з точки зору суспільних інтересів, ця інформація має бути відома громадськості. В цьому випадку має місце конфлікт інтересів: для фірми поява правдивої інформації щодо її діяльності буде негативним інформаційним впливом, тоді як для громадськості – безперечно позитивним [*2*].

Окремої уваги заслуговує питання захисту свідомості людини від деструктивного інформаційного впливу. Соціально-філософська проблематика цієї теми досить глибока, тому зараз ми лише у загальних рисах окреслимо основні моменти.

Значне посилення інформаційного навантаження, різка зміна культурної парадигми, руйнування загальноприйнятої системи ідеологічних координат призводять до дезадаптації людини, виникнення труднощів у осмисленні соціальної реальності. В той же час сучасний світ вимагає постійного включення, інтелектуальної активності людини, адже кожний новий день може принести важливу інформацію та змінити «правила гри», а нетривале випадення з інформаційного струменя, може призвести до серйозної і тривалої втрати позицій.

Із збільшенням кількості інформаційних каналів розширюються можливості маніпулювання суспільною та індивідуальною свідомістю, розвиваються техніки та методи управління громадською думкою. Посилення інформаційної нерівності призводить до того, що люди, які не мають повноцінного доступу до сучасних технологій, різнобічної інформації, нових знань та баз даних, стають значно уразливішими перед впливом краще забезпечених осіб, які можуть обмежувати інформацію та представляти її в дозованій формі. У разі застосування відповідних прийомів та технік це дозволяє сформувати шаблони сприйняття інформації, спрямувати ментальну діяльність та поведінку людей у необхідне русло.

За певних умов наслідком деструктивного інформаційного впливу може бути масове поширення феномену керованої стереотипами, програмованої людини, деактуалізація особи та деградація суб'єктності як здатності людини до формування власної позиції та творчої самореалізації через недостатній розвиток свідомості та соціальної рефлексії.

Як бачимо, інформаційна безпека є складним багатоаспектним феноменом, який потребує великої уваги як з боку науковців-теоретиків, так і практиків, причому основний акцент слід зробити на питанні захисту найбільш вразливої і малодослідженої ланки в системі інформаційної безпеки – на питанні захисту людської свідомості від деструктивного інформаційного впливу.

ЛІТЕРАТУРА

1. *Про Основні засади* розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 9 січня 2007 року № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст.102.
2. *Архипов О. Є., Архипова Є. О.* Положення про інформаційну безпеку в міжнародних стандартах / О.Є. Архипов, Є.О. Архипова // Інформаційна безпека людини, суспільства, держави. – 2010. – № 2 (4). – С. 62-65.
3. *Василюк В. Я., Климчик С. О.* Інформаційна безпека держави / В. Я. Василюк, С. О. Климчик. – К.: КНТ; ВД «Скіф», 2008. – 136 с.
4. *Інформаційна* безпека людини, суспільства, держави: наук.-практ. ж-л / НА СБУ. – 2009. – № 1 (1). – 106 с.
5. *Лужецький В. А., Войнович О. П., Дудатьєв А. В.* Інформаційна безпека: навч.посіб. / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.
6. *Скиба В. Ю., Курбатов В. Я.* Руководство по защите от внутренних угроз информационной безопасности / В.Ю. Скиба, В.Я. Курбатов. – СПб.: Питер, 2008. – 320 с.
7. *ISO/IEC* 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.

Стаття надійшла до редакції 30.11.2011 р.