

УДК

Наталія Миколаївна Волошина

## ПОНЯТТЯ “БЕЗПЕКА ІНФОРМАЦІЇ” ТА “ІНФОРМАЦІЙНА БЕЗПЕКА” В СУЧАСНОМУ НАУКОВОМУ ПРОСТОРІ

**Актуальність теми.** В теперішній час інформація перетворилась у формуючий фактор матеріального середовища життя людини, виступаючи у ролі інноваційних технологій, комп'ютерних програм тощо. Водночас вона використовується як основний засіб міжособистісної взаємодії, постійно виникаючи та змінюючись у процесі переходу від однієї інформаційної системи до іншої. Таке становище інформації в суспільстві обумовлює необхідність відноситись до неї як до товару, що має певну цінність, зростаючи залежно від достовірності, корисності й доступності. Доступність робить інформацію найпривабливішою, оскільки її конфіденційність обмежується колом осіб, наділених правом володіти нею. Захист інформації, віднесеної до державної таємниці, слід вважати невід'ємною складовою національної безпеки України.

За роки незалежності України реалізовано комплекс заходів щодо вдосконалення законодавчої та нормативно-правової бази гарантування інформаційної безпеки. Вчені Національного технічного університету України “КПІ” підрахували, що безпосередньо або побічно з питань інформаційної безпеки на 1 січня 2001 року в Україні було прийнято 257 законів України, Постанов Верховної ради України нормативного характеру — 290, Указів і розпоряджень президента України відповідно — 368 і 87, постанов Кабінету міністрів України — 1149, нормативно-правових актів міністерств і відомств — 1095 [1, с. 32—41]. За останні вісім років за неповними даними, було прийнято 15 законів, 14 Указів Президента України, 41 Постанова Кабінету міністрів України і близько 50 нормативно правових актів Державної служби спеціального зв'язку та захисту інформації України [2, с. 39]. Це свідчить про злободенність і актуальність дослідження питань інформаційної безпеки. Кількість законодавчих і нормативно-правових актів свідчить про необхідність

осмислення і порівняння понять “безпека інформації” та “інформаційна безпека”.

**Мета** статті — дослідити соціально-філософський вимір інформаційної безпеки України. Для реалізації визначеної мети в статті вирішуються наступні **завдання**: 1) здійснюється соціально-філософський аналіз поглядів на сутність інформації; 2) зіставляється зміст понять “безпека інформації” та “інформаційна безпека”; 3) простежуються значущі інформаційні загрози сучасності.

Термін *інформація* походить від латинського *informatio* і перекладається буквально: ознайомлення, роз'яснення, уявлення, поняття. Можна обмежитись даним визначенням терміну *інформація* оскільки в більшості наукових праць з проблем інформаційної безпеки, поняття *інформація* взагалі не формулюється. З іншого боку, аналіз наукової літератури свідчить про наявність у сучасній літературі безлічі визначень сутності інформації, серед яких можна виділити чотири принципових підходи.

По-перше, академік В. Глушков вважав, що інформація є атрибутом (невід'ємною властивістю) не тільки живих, розумних істот, але й усіх матеріальних тіл [3, с.126]. Інформація у неорганічній природі існує об'єктивно, але як би в потенційній формі. З появою живих організмів, тобто споживачів інформації, починається використання інформації з метою пізнання й управління. Отже, інформація, будучи атрибутом матерії й руху, існує споконвічно в просторі й часі.

По-друге, засновник кібернетики Н. Вінер стверджував, що інформація є властивістю лише високоорганізованої, тобто живої матерії. Інформація й інформаційні процеси, на його думку, властиві тільки біологічній і соціальній формам руху матерії. Він вважав, що живі організми розвивають необхідну їм інформацію завдяки постійній взаємодії із природою, обміну з навколишнім середовищем [4, с.69]. При цьому інформації належить особлива інтег-

руюча роль, завдяки якій у живих істот й, насамперед у людини, розвилися адаптаційні здібності. У такий спосіб інформація лежить в основі процесів саморегулювання у живій природі.

По-третє, К. Шеннон пропонує функціональний підхід до розуміння сутності інформації, у рамках якого інформацію часто розглядають як властивість лише систем, що самоорганізуються, не тільки у живій природі, але й у техніці. До них, наприклад, відносять і живі істоти й кібернетичні системи, для яких характерні процеси саморегулювання завдяки передаванню, зберіганню й переробленню інформації [5, с.84].

По-четверте, В. Афанасьєв пропонує ще й соціальний підхід до інформації. Він розуміє інформацію як продукт життєдіяльності тільки соціальних форм матерії, людського суспільства. Інформація існує об'єктивно в просторі й часі, але проявляється лише в процесі пізнання людиною навколишнього світу [6, с.35].

Особливе значення серед соціальних теорій інформації має семіотична концепція. Головною проблемою інформаційних зв'язків і систем у суспільстві є проблема мови, яку можна розглядати як семіотичну систему знаків, символів і правил, за допомогою яких відображається й передається інформація.

Так, з позицій семіотики, будь-яка інформація (повідомлення) є не що інше як набір знаків й, отже, може розглядатися з позицій семантичних, синтаксичних і прагматичних характеристик.

Синтаксис вивчає систему правил у мові, за якими із знаків побудовані речення й вислови. Семантика — це вчення про зміст слів. Зміст слова, як відомо, передається через поняття. Семантика вивчає точність відтворення в інформації сутності віддзеркаленого явища, тобто його змісту. У свою чергу, прагматика вивчає зв'язки між знаками й людьми, які ці знаки встановлюють й вживають. Вона встановлює зв'язок змісту повідомлення й мети діяльності або управління, корисність, важливість, роль і значення інформації для конкретних справ, тобто цінність інформації.

Цим трьома частинами лінгвістики відповідають три аспекти інформації: синтаксичний (формальний), семантичний (змістовний) і прагматичний (ціннісний). Інформація, що виходить від об'єкта-оригіналу й сприймається суб'єктом-споживачем в інтересах тієї або іншої діяльності, кодується й передається людиною за допомогою мови, що містить не тільки формальні (кількісні), але й змістовні (якісні) характеристики, віддзеркалені синтаксис-

ом, семантикою й прагматикою. Відповідно до семіотичної теорії, тільки їхня єдність виражає сутність інформації. Таким чином, інформація за семіотикою — це кодовані за допомогою знакових систем і передані для використання в спілкуванні людьми відомості, повідомлення, дані в сполученні синтаксичних, семантичних і прагматичних характеристик.

У сучасній системі наукових знань мають місце й інші теорії, які пояснюють сутність інформації, що свідчить про граничну узагальненість, складність і багатогранність цього явища. Слід зазначити, що в системі наукових знань відсутнє універсальне поняття інформації. Відсутність єдиного розуміння даного явища призвело до безлічі його дефініцій.

Вважаємо за доцільне з безлічі визначень інформації надати найбільш популярні формулювання: «інформація є інформація, не матерія й не енергія» (Вінер); «це позначення змісту, отриманого від зовнішнього світу в процесі пристосування до нього» (Вінер); «повідомлення, освідомлення про положення справ, навчання, відомості про будь-що передані людьми» (Бріллюєн); «комунікація й зв'язок, у процесі якої усувається невизначеність» (Шеннон); «передача розмаїтості» (Ешбі); «оригінальність, новизна; міра складності структур» (Моль); «здатність знаків викликати образи» (Ягль); «передача, відбиття розмаїтості в процесах й об'єктах» (Урсул); «повідомлення про якісь події, чийсь діяльність; відомості, що є об'єктом зберігання, накопичення, переробки і передавання» (Словник іншомовних слів). Це всього лише мала частина визначень інформації, що розкривають ту або іншу грань даного феномена. На думку вчених, інформація має деякі загальні специфічні властивості: вона принципово не створюється й не знищується, а всього лише виникають (нові ідеї, знання), передається й приймається, так само як руйнується, губиться й забувається; при цьому вона може змінювати форму, не змінюючи свого змісту; на відміну від інших ресурсів вона може бути використана багаторазово істотно не зношуючись.

Виходячи із наукових підходів і законодавчих актів України, пропонується визначити інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. Інформацією можна вважати дані, що знайшли власного споживача.

Вся інформація, що створюється і поширюється в нашій державі, незалежно від змісту, форм, часу й місця становить її інформаційні ресурси. Україна самостійно

формує інформаційні ресурси на своїй території та вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами. Національні інформаційні ресурси є основою інформаційного суверенітету України, який гарантується інформаційною безпекою.

Питання інформаційної безпеки знаходиться в центрі уваги вчених. Про це свідчить значна кількість монографій наукових статей у відкритих часописах. Це роботи В. Богуша, І. Замаруєвої, М. Згуровського, Я. Жаркова, В. Остроухова, О. Рося і багатьох інших. Значну частку наукових праць вітчизняних авторів присвячено всебічному аналізу інформаційної безпеки. При цьому дещо поза увагою залишається безпека інформації. На перший погляд, “безпека інформації” та “інформаційна безпека” тотожні за змістом, але насправді це далеко не відповідає істині. В першому випадку об’єктом є інформація, в другому — безпека як частина цілої національної безпеки.

Розглянемо поняття “безпека інформації”. Воно є поліаспектним. По-перше, безпека інформації за суттю є стан інформації, інформаційних ресурсів та інформаційних і телекомунікаційних систем, при якому з необхідною вірогідністю забезпечується захист інформації. По-друге, це стан захищеності інформації, що обробляється засобами обчислювальної техніки або автоматизованої системи від внутрішніх та зовнішніх загроз.

Безпека інформації забезпечується шляхом захисту інформації від випадкового або навмисного доступу осіб, що не мають на це права, її здобуття, розкриття, модифікації або руйнування. Реалізація вимог і правил щодо захисту інформації, підтримки інформаційних систем в захищеному стані, експлуатації спеціальних технічних і програмно-математичних засобів захисту і забезпечення організаційних і інженерно-технічних заходів захисту інформаційних систем, що оброблюють інформацію з обмеженим доступом в недержавних структурах, здійснюється службами безпеки інформації. Створення розгалужених інформаційних мереж, пов’язаних із банківською системою обумовило необхідність захисту інформації за допомогою: додаткових засобів ідентифікації й аутентифікації обличчя, запровадження системи (PIN-код, інформації про клієнта на магнітній смужі в пам’яті мікросхеми картки, шифрування даних, контрольні числа й інші засоби захисту карток), засобів криптозахисту інформації в каналах зв’язку і т.п. Епоха “інформаційної супермагістралі”: вибухоподібний розвиток мережі Internet і

зв’язаних з нею послуг обумовили необхідність створення принципово нової системи безпеки інформації. На сьогодні склалися два підходи до забезпечення безпеки електронних систем: фрагментарний підхід, при якому здійснюється протидія строго визначеним загрозам при певних умовах (спеціалізовані антивірусні засоби, автономні засоби шифрування, тощо); комплексний підхід, який передбачає створення середовища обробки інформації, що об’єднує різноманітні (правові, організаційні, програмно-технічні) заходи для протидії загрозам. Комплексний підхід, як правило, використовується для захисту великих систем. Хоча часто і типові програмні засоби містять вбудовані засоби захисту інформації, але цього замало.

Для гарантування безпеки інформаційних систем прямо чи опосередковано пов’язаних з адміністративним управлінням вживаються наступні заходи: фізичний захист комп’ютерних систем; регламентація технологічних процесів; регламентація роботи з конфіденційною інформацією; регламентація процедур резервування; регламентація внесення змін; регламентація роботи персоналу і користувачів; заходи контролю і спостереження. Для систематизації захисту інформації її поділено на наступні категорії: а) важлива інформація — не замінима та необхідна для діяльності, процес відновлення якої після знищення неможливий або ж дуже трудомісткий і пов’язаний з великими затратами, а її помилкове застосування чи підробка призводить до великих втрат; б) корисна інформація — необхідна для діяльності, яка може бути відновлена без великих втрат, при чому її модифікація чи знищення призводить до відносно невеликих втрат; в) конфіденційна інформація, доступ до якої для частини персоналу або сторонніх осіб небажаний, оскільки може спричинити матеріальні та моральні втрати; г) відкрита інформація — це інформація, доступ до якої відкритий для всіх. У є певні нормативні акти, які визначають категорію інформації та спеціальні державні і недержавні структури, що здійснюють нагляд за безпекою інформації.

Інформаційної безпека є невід’ємною частиною національної безпеки. Що вона являє собою? Найточніше визначення поняття “інформаційна безпека” сформульовано в двох законах “Про основні засади розвитку інформаційного суспільства в Україні на 2007—2015 рр.” [8] та “Про захист життєво важливих інтересів людини, суспільства і держави, при якому попередження нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформа-



ційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації". В другому документі інформаційна безпека ототожнюється із інформаційною безпекою телекомунікаційних мереж. На превеликий жаль в інших законах визначення змісту інформаційної безпеки не здійснено. Інколи поняття інформаційна безпека підміняється терміном "національна безпека в інформаційній сфері". Основними аспектами інформаційної безпеки стосовно до будь-якої інформаційної системи є доступність, цілісність і конфіденційність.

На підставі аналізу законодавчої, нормативно-правової бази та наукових підходів до аналізу інформаційної безпеки пропонується визначити її як захищеність встановлених законодавчо інформаційних процесів в державі, що забезпечують гарантовані Конституцією України умови розвитку людини, суспільства й держави, середовища суспільства, яке забезпечує її використання і розвиток на користь громадян, організацій, держави.

Співставлення понять *безпека інформації* та *інформаційна безпека* дозволяє дійти **висновку**, що друге поняття значно глибше за сутністю і ширше за змістом. Інформаційну безпеку України можна розглядати з позицій захисту не тільки інтересів держави, а насамперед особистості й суспільства. Окрім цього інформаційну безпеку, на думку В. Петрика, можна також досліджувати в контексті захисту інформаційних технологій, інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов для існування й розвитку інформаційних процесів [9, с. 47].

Оскільки розмова йде про захист, логічно буде з'ясувати від яких загроз слід захищати особистість, суспільство та державу. Загально прийнятим у науковому середовищі під загрозами розуміти дію або бездіяльність конкретних осіб, які призводять до спотворення, знищення поширення конфіденційної інформації, створення небезпечних умов для інформаційних процесів та інформаційних технологій.

До загроз інформаційній безпеці пропонується віднести наступні: прояви обмеження свободи слова та доступу громадян до інформації; комп'ютерну злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Таким чином, інформація є формою реального буття. Вона існує на біологічному, фізіологічному, соціальному, механічному, фізичному, хімічному рівнях. Соціальною інформацією називаються спожиті суб'єктом соціальної діяльності документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Безпека інформації за суттю є стан інформації, інформаційних ресурсів та інформаційних і телекомунікаційних систем, при якому з необхідною вірогідністю державними і недержавними структурами забезпечується захист інформації від внутрішніх або зовнішніх загроз.

## Література

1. **Правове**, нормативне та метрологічне забезпечення системи захисту інформації в Україні : Зб. наук. праць НТУУ "КПІ". — К. : НТУУ "КПІ", 2000. — № 1. — С. 32—41.
2. **Безпека** сталого розвитку України: побудова в умовах глобальних викликів : монограф. / за ред. В. О. Ананьїна. — К. : ІСЗІ НТУУ "КПІ", 2009. — 271 с.
3. **Глушков В. М.** Человек и вычислительная техника / В. М. Глушков. — К. : Наук. думка, 1971. — 418 с.
4. **Винер Н.** Кибернетика, или Управление и связь в животном и машине / пер. с англ. — М. : Прогресс, 1972. — 273 с.
5. **Шеннон К. Э.** Работы по теории информации и кибернетики / К. Э. Шеннон. — М. : Прогресс, 1963. — 298 с.
6. **Афанасьев В. Г.** Социальная информация и управление обществом / В. Г. Афанасьев. — М. : Наука, 1975. — 316 с.
7. **Закон** України "Про основні засади розвитку інформаційного суспільства в Україні на 2007—2015 роки" // Відомості Верховної ради України. — 2007. — № 12. — Ст. 102.
8. **Закон** України "Про телекомунікації" // Відомості Верховної ради України. — 2007. — № 12. — Ст. 155.
9. **Галамба М.** Інформаційна безпека України: поняття, сутність та загрози // М. Галамба, В. Петрик. — Юрид. журнал. — 2006. — № 11. — С. 35—47.

В статье рассматривается сущность понятий *информация*, *безопасность информации*, анализируются научные подходы к пониманию информационной безопасности, актуализируются угрозы информационной безопасности.

**Ключевые слова:** информация, безопасность информации, информационная безопасность, угрозы информационной безопасности.