УДК: 004.056.5 (303.01)

ТИХОМИРОВ Олександр Олександрович

ІНФОРМАЦІЙНА БЕЗПЕКА: СОЦІОТЕХНІЧНА ПАРАДИГМА

Постановка проблеми. Упровадження новітніх інформаційних технологій базується на активному застосуванні методів і засобів кібернетики в багатьох сферах життєдіяльності людини, значно підвищує її інформаційний потенціал, закладаючи тим самим фундамент глобального інформаційного суспільства.

Сучасні розвинені країни із кожним днем просуваються на шляху становлення інформаційного суспільства, що зумовлює кардинальні зміни суспільних відносин у багатьох сферах, зокрема політиці, економіці, управлінні, освіті, науці.

Реалізація функцій сучасної держави у цих сферах, а також виконання завдань забезпечення безпеки суспільства залежить від розвиненості і надійності інформаційно-телекомунікаційних мереж, систем зв'язку й управління, їх програмного та апаратного забезпечення, які становлять технічну основу інформаційної інфраструктури й одночасно зумовлюють її вразливість.

Світовий досвід свідчить, що загрози, які існують у сучасному інформаційному просторі, мають переважно глобальну природу, високу динаміку і латентність, спонтанність виникнення і розвитку, внаслідок чого суттєво ускладнюють і певною мірою обмежують існуючі суспільні механізми (зокрема державні і правові) їх попередження, подолання, усунення чи мінімізацію небезпечних наслідків.

Саме тому інформаційна безпека як актуальний об'єкт наукового пізнання вийшла поза межи суто технічної науки і зумовила предметне спрямування численних соціально-гуманітарних наукових досліджень, сформувавши окрему комплексну галузь знань. Проте слід визнати, що в Україні розвиток цієї галузі певним чином гальмується відсутністю єдиної наукової спеціальності, яка б об'єднала у собі напрями як технічних, так і деяких соціально-гуманітарних (філософських, правових, психологічних тощо) дисертаційних досліджень, безпосереднім об'єктом яких є інформаційна безпека і проблеми її забезпечення.

Аналіз останніх досліджень і публікацій. Очевидно, що природу сучасних інформаційних перетворень суспільства визначає науково-технічний прогрес. Тому природною є і первинність щодо них саме технічно орієнтованої наукової думки, спрямованої на моделювання, аналіз прогнозування, інформаційних процесів, інформаційно-аналітичної підтримки процесів прийняття рішень

тощо в різноманітних системах за допомогою математичних методів.

Ці властивості сучасних інформаційних загроз зумовили їх наукове осмислення не тільки в технічних, а й у правових та інших соціально-гуманітарних науках.

Так, не заперечуючи авторського вкладу усіх дослідників інформаційного напряму, у межах цієї публікації варто виокремити праці таких авторів:

– у фундаментальній правовій науці – В.М.Лопатіна, Ю.Є.Максименко, Т.А.Полякова, А.О.Стрельцова, які досліджували теоретико-правові аспекти забезпечення інформаційної безпеки в контексті взаємозв'язків із відповідними державними і правовими явищами;

– у галузевих і прикладних правових науках на проблемах інформаційної безпеки акцентували свою увагу у межах: адміністративно-правового забезпечення – І.В.Арістова, К.І.Бєляков, Б.А.Кормич, О.В.Логінов; кримінально-правової охорони – Д.С.Азаров, В.М.Бутузов; інформаційного права – О.А.Баранов, Р.А.Калюжний, А.І.Марущак, В.С.Цимбалюк, М.Я.Швець; криміналістики – А.С.Білоусов, Л.В.Борисова, А.Т.Журба, Д.В.Пашнєв; цивільного права – В.С.Дмитришин, А.С.Колісник, О.В.Кохановська;

– у спеціальних правових дослідженнях інформаційну безпеку в контексті національної безпеки, міжнародних стандартів її забезпечення осмислювали В.Ю.Артемов, В.П.Горбулін, О.Г.Данільян, О.П.Дзьобань, Г.В.Іващенко, В.А.Ліпкан, Г.В.Новицький, М.І.Панов;

– в інших соціально-гуманітарних науках філософсько-соціологічні аспекти забезпечення інформаційної безпеки розглядали – Я.С.Артамонова, М.Ю.Захаров, О.М.Циденова; політологічні – М.І.Бусленко, В.К.Конах, О.О.Ніколаєв; психологічні – Г.В.Грачов, С.Кара-Мурза, О.М.Морозов, В.В.Остроухов, І.Н.Панарін, В.М.Петрик, Г.Г.Почепцов.

При цьому, незважаючи на існуючі науково-організаційні проблеми в Україні де-факто існує відносно відокремлений комплексний напрям – спеціалізовані дослідження інформаційної безпеки, розвитку якого сприяють М.М.Галамба, О.О.Климчук, В.А.Ліпкан, В.М.Панченко, В.І.Полевий, О.М.Солодка та інші.

Метою статті є поглиблення міждисциплінарних (міжгалузевих) зв'язків наукових знань про інформаційну безпеку, передусім соціально-гуманітарних, шляхом сприяння формуванню і розвитку соціотехнічної парадигми інформаційної безпеки.

Виклад основного матеріалу. Значна частина гносеологічних проблем інформаційної безпеки лежить у площині аналогічних проблем безпеки як явища. Специфічність наукових підходів "дисциплінарних" фахівців до осмислення інформаційної безпеки та форм і методів її забезпечення ґрунтуються на особливостях сприйняття базового поняття "безпека" відповідною галуззю знань. Зважаючи на те, що безпека є складним соціально-політичним феноменом, необхідна інтеграція теоретико-методологічних здобутків різних наук щодо розкриття її змісту.

Так, психологи визначають її як відчуття, сприйняття і переживання

необхідності у захисті життєво важливих потреб і інтересів людини; юристи (правники) – як систему встановлених законом правових гарантій захищеності особи і суспільства, забезпечення їх нормальної життєдіяльності, прав і свобод; філософи – як стан, тенденції розвитку й умови життєдіяльності соціуму та його структур, за яких забезпечується збереження їх якісної визначеності та оптимальне співвідношення свободи і необхідності; політологи – як властивість (якість) системи і результат діяльності низки систем і органів держави, а також сам процес діяльності, спрямованої на досягнення визначених завдань щодо забезпечення захищеності особи, суспільства, держави [1, с. 46-47].

Аналогічна інтегративна концепція прийнятна і для інформаційної безпеки. Причому вона матиме визначену природою інформаційної безпеки яскраво виражену технікотехнологічну складову, яку доцільно інтерпретувати через достатність і надійність усіх компонентів технічних систем обробки, обміну, зберігання інформації, що забезпечує їй бажані властивості (цілісність, доступність, конфіденційність, спостережність тощо).

Сьогодні вирішення проблеми формування єдиної концепції інформаційної безпеки викликає певні труднощі, зумовлені низкою факторів, зокрема недостатньою розробленістю методологічних основ інформаційної теорії загалом, а не тільки теорії інформаційної безпеки, необхідністю трансформації в контексті інтеграції вже збудованих методологічних основ окремих її складових, несформованістю єдиного змістового наповнення центрального інтегруючого поняття "інформаційна безпека".

Варто погодитися із науковцями, які вбачають підґрунтя вирішення цієї проблеми у виявленні загального та відмінного базових складових сучасної інформаційної теорії – теорії інформаційної безпеки, теорії соціотехнічних систем, теорії права інформаційного суспільства [2].

Сучасна концепція соціотехнічних систем у протиставлення теорії технологічного детермінізму, яка стверджує односторонню дію технології на людину, ґрунтується на ідеї взаємодії людини і техніки, тобто на взаємозалежних впливах [3]. До підсистем соціотехнічної системи належать: технічна підсистема, яка містить пристрої, інструменти і технології перетворення інформації (даних) із метою покращання ефективності функціонування системи; соціальна підсистема, яка включає людей (суб'єктів), їх індивідуальні можливості, знання, уміння, ціннісні установки, психофізіологічні властивості, стимули, відношення до виконуваних функцій, управлінську структуру тощо.

Таким чином, головні об'єкти безпеки, зокрема й інформаційної, – людина (організації людей), суспільство, держава в сучасних умовах інформатизації мають усі ознаки соціотехнічних систем.

Захищеність соціотехнічних систем визначається ефективністю реагування системи забезпечення інформаційної безпеки на існуючі загрози. Оскільки життєдіяльність усіх соціотехнічних систем проходить у певному

середовищі – навколишньому, економічному, технологічному, інформаційному тощо, у процесі взаємодій між ними може виникати конкуренція і відповідні взаємні впливи. В інформаційному середовищі можуть активно використовувати сучасні технології інформаційної війни, проявами яких є конкурентна розвідка, промислова розвідка, "чорний" PR тощо [3-5].

Отже, трансформуючи інформаційну безпеку крізь призму теорії соціотехнічних систем, можна достатньо чітко виокремити три її складові: перша визначається технічними, технологічними можливостями суб'єктів в інформаційній сфері (технікотехнологічна складова), друга – індивідуальними якостями суб'єктів щодо сприйняття інформації і реакції на неї (інформаційно-психологічна складова), третя – упорядкованістю, організованістю суспільних інформаційних відносин (правова складова).

Така триєдність інформаційної безпеки відзначається й окремими правовими дослідженнями. Так, Ю.Є.Максименко, проаналізувавши на дисертаційному рівні теоретико-правові засади забезпечення інформаційної безпеки України, трактує її як інформаційну безпеку у сфері прав і свобод людини і громадянина, інформаційно-технічну й інформаційно-психологічну безпеку [6].

Іншими важливими складовими підґрунтя соціотехнічної парадигми інформаційної безпеки може стати низка таких теоретичних орієнтирів.

1. З огляду на гуманітарну парадигму безпеки, яка простежується на концептуально-доктринальному рівні законодавства (зокрема у нормативно-правових актах щодо національної безпеки в Україні), однією із її невід'ємних гносеологічних властивостей є суб'єктивність, тобто неможливість осмислення безпеки безвідносно певного суб'єкта. Інформаційна безпека як одна із складових (видів, компонентів) загальної (загальносоціальної, національної тощо) безпеки отримує таку ж властивість. При цьому інформаційна безпека окремого індивіда значною мірою залежить від інформаційної безпеки суспільства, держави, оскільки всі ці суб'єкти взаємопов'язані у процесі забезпечення інформаційної безпеки кожного із них.

Така інтерпретація інформаційної безпеки вимагає певного переосмислення деяких загальнопоширених понять, які мають переважно технічну природу походження, а саме понять "безпека інформації", "безпека комп'ютерної системи", "безпека системи автоматизованої обробки інформації", "безпека інформаційно-комунікаційних технологій" тощо.

Ці поняття за своїм змістом мають не суб'єктне, а об'єктне спрямування, оскільки виходять із суто технічного сприйняття інформаційної безпеки як системи заходів із захисту інформації щодо певного об'єкта, у межах якого здійснюється оброблення інформації. Змістом безпеки у цьому ракурсі стають необхідні якості або характеристики об'єктів безпеки, на здобуття яких спрямовані відповідні захисні заходи. Такими якостями інформації є цілісність, доступність, конфіденційність, спостережність, а комп'ютерних систем – дос-

татність, надійність, оптимальність, контрольованість тощо.

Проте сучасне уявлення про забезпечення інформаційної безпеки значно ширше за захист інформації, який визнається одним із його напрямів, що не дозволяє їх ототожнювати. Крім того, інформація сьогодні розглядається як соціальна цінність, а отже нерозривного пов'язана із певним суб'єктом, для якого вона є такою цінністю. Це дає змогу стверджувати про доцільність наукового розгляду інформаційної безпеки відносно певного суб'єкта (частиною якого є належна йому інформація), а не відносно несуб'єктивізованої інформації.

2. З одного боку, заглиблюючись у філософію, можна говорити про "ілюзію безпеки" як сукупність індивідуальних властивостей суб'єктів, які дозволяють їм функціонувати у певних умовах. При цьому в інформаційному середовищі, враховуючи глобальність, динамічність, латентність та необмеженість форм прояву інформаційних загроз, безпека буде найбільш "ілюзорною". З іншого – важливо встановити певний узагальнений бажаний рівень безпеки – "стандарт безпеки", визначення і досягнення якого справа соціальних інститутів державного, регіонального і світового рівня.

3. Розглядаючи об'єкти інформаційної безпеки як соціотехнічні системи, а їх захищеність як належну реакцію на дестабілізуючі впливи, інформаційну безпеку доцільно сприймати через діяльнісну модель, тобто як цілеспрямовану діяльність, невід'ємними змістовими компонентами якої є мета і завдання, суб'єкти й об'єкти, засоби і методи, принципи, результати.

Слід зазначити, що діяльнісний підхід дає змогу гармонійно поєднати у собі основні існуючі напрями розуміння інформаційної безпеки, зокрема як управління загрозами, як системи захисних заходів, захищеності, умов функціонування (життєдіяльності) суб'єктів в інформаційному середовищі, оскільки всі вони можуть бути інтерпретовані через певні змістові компоненти діяльності [7; 8].

Таким чином соціотехнічна парадигма як міждисциплінарна система ідей охоплює значну сферу уявлень про інформаційну безпеку і процеси її забезпечення.

У межах соціотехнічної парадигми умовно інформаційну безпеку можна структурувати не тільки за складовими, а й за рівнями, утворюючи трирівневу і трискладову модель, зображену на рис. 1.

1) *Індивідуальний рівень* – це здатності, можливості, навички суб'єктів в інформаційній сфері, зокрема у сфері особистого захисту від інформаційних загроз.

Серед компонентів технікотехнологічної складової індивідуального рівня:

– можливості вільного доступу до інформаційних ресурсів;

– забезпеченість сучасними засобами обробки інформації;

– уміння і навички сучасної технічної обробки інформації.

Компоненти правової складової індивідуального рівня:

– загальна правова культура і правосвідомість;

– здатності адекватного сприйняття правової інформації;

– орієнтованість на захист власних прав і свобод.

Компоненти інформаційно-психологічної складової індивідуального рівня:

– загальний інтелектуальний розвиток і моральність;

– сформованість інформаційних потреб;

– усвідомленість інформаційних загроз;

– здатності критичного ставлення до інформації;

– динамічність свідомості.

Рис. 1. Структуризація інформаційної безпеки за складовими і рівнями

2) *Загальний рівень* – умови, які безпосередньо визначають інформаційну розвиненість і створюють інформаційне середовище функціонування суб'єктів.

Компоненти техніко-технологічної складової загального рівня:

– розвиток технічної бази інформаційного простору;

– розвиток інформаційно-телекомунікаційних технологій.

Компоненти правової складової загального рівня:

– упорядкованість важливих видів інформаційної діяльності;

– затвердження концептуальних начал в інформаційній сфері;

– адекватна урегульованість суспільних відносин в інформаційній сфері;

– визначеність і визнання прав і свобод людини в інформаційній сфері;

– законність і правопорядок в інформаційній сфері.

Компоненти інформаційно-психологічної складової загального рівня:

– позитивний (сприятливий) морально-психологічний клімат;

– збереження національної ідентичності;

– популяризація національної культури;

– позитивний імідж суспільства на міжнародній арені.

3) *Рівень захисту (захисний рівень)* – система захисних механізмів в інформаційній сфері.

Компоненти техніко-технологічної складової рівня захисту:

– технічний захист певних категорій інформації;

– криптографічний захист певних категорій інформації;

– технічні засоби ідентифікації й аутентифікації;

– процедури забезпечення надійності і достатності технічних систем обробки інформації.

Компоненти правової складової рівня захисту:

– заборони і юридична відповідальність у сфері інформаційних правовідносин;

– упорядкування захисту певних категорій інформації (в Україні – інформація з обмеженим доступом);

– упорядкування використання спеціальних засобів отримання інформації;

– регламентація психологічного захисту свідомості людини, суспільства.

Компоненти інформаційно-психологічної складової рівня захисту:

– механізми протидії маніпулюванню свідомістю шляхом надання викривленої, недостовірної, неповної інформації або шляхом використання сугестивних технологій і, зокрема, нейролінгвістичного програмування.

Звичайно перелік цих компонентів невичерпний, оскільки його спрямовано виняткова на обрану у цій публікації концепцію осмислення інформаційної безпеки.

Висновки. Сьогодні інформаційна безпека утворює одну із фундаментальних основ розвитку суспільства. Від повноти її сприйняття безпосередньо залежить якість організації діяльності із забезпечення інформаційної безпеки, зокрема адекватність визначення мети і завдань цієї діяльності, оптимальність вибору методів і засобів, відповідність отриманих результатів тощо. Соціотехнічна парадигма інформаційної безпеки має інтегративний потенціал, здатний консолідувати різні наукові позиції щодо неї шляхом формування єдиної комплексної галузі знань про інформаційну безпеку, що сприятиме об'єктивності й обґрунтованості результатів наукових досліджень, посиленню їх практичної значущості, і в підсумку, підвищенню ефективності системи забезпечення інформаційної безпеки.

Список використаних джерел

1. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / А.А.Стрельцов. – М. : МЦМНО, 2002. – 296 с.

2. Фисун А.П. Различия и единство методологии теорий информатики, информационной безопасности социотехнических систем и теория права информационного общества: проблемы формирования информационной теории [Электронный ресурс] / А.П.Фисун, Ю.А.Белевская. – Режим доступа : http://itnop.ostu.ru.

3. Дудатьєв А.В. Інформаційна безпека соціотехнічних систем в умовах інформаційної війни / А.В.Дудатьєв // Інформаційні технології та комп'ютерна інженерія. – 2011. – № 3. – С. 75-79.

4. Дудатьєв А.В. Аксіоматика теорії комплексної безпеки соціотехнічних систем / А.В.Дудатьєв // Інформаційні технології та комп'ютерна інженерія. – 2013. – № 1. – С. 22-25.

5. Дудикевич В.Б. Моделювання інформаційно-психологічних операцій в соціотехнічних системах / В.Б.Дудикевич, Ю.Р.Гарасим, І.М.Цвяк // Вісник Східноукраїнського національного університету ім. В.Даля. – 2010. – № 9 (151). –Ч. 1. – С. 130-135.

6. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. … канд. юрид. наук : 12.00.01 / Ю.Є.Максименко. – К., 2007. – 186 с.

7. Тихомиров О.О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: об'єкти і суб'єкти / О.О.Тихомиров // Інформаційна безпека людини, суспільства, держави. – 2012. – № 2 (9). – С. 18-24.

8. Тихомиров О.О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: мета, засоби і методи, принципи, результати / О.О.Тихомиров // Інформаційна безпека людини, суспільства, держави. – 2012. – № 3 (10). – С. 11-17.

Аннотация: Статья посвящается формированию социотехнической парадигмы информационной безопасности, что на общетеоретическом уровне будет способствовать гармонизации и системности научных исследований в разных отраслях знаний, частью предметной сферы которых являются проблемы информационной безопасности.

Ключевые слова: информационная безопасность, составляющие информационной безопасности, правовая защита информации, техническая защита информации, информационно-психологическая защита.

Abstract: The article considers formation of social and technical paradigm information security that on the general theoretical level will contribute to the harmonization and systematization of scientific research in the different brunches of knowledge, the part of objective spheres of which is the problems of information security.

Key words: information security, components of information security, legal protection of information, technical protection of information, information and psychological protection.