РОЗВИТОК ПРОДУКТИВНИХ СИЛ
І РЕГІОНАЛЬНА ЕКОНОМІКА

УДК 332.146.2:330.47

DOI: https://doi.org/10.32782/2520-2200/2019-5-25

Дубницький В.І.
доктор економічних наук, професор, академік АЕН України,
професор кафедри теоретичної та прикладної економіки
Державного вищого навчального закладу
«Український державний хіміко-технологічний університет»
Науменко Н.Ю.
кандидат технічних наук, доцент,
доцент кафедри теоретичної та прикладної економіки
Державного вищого навчального закладу
«Український державний хіміко-технологічний університет»

Dubnitskyi Volodymyr
State Higher Education Institution
"Ukrainian State University of Chemical Technology"
Naumenko Nataliia
State Higher Education Institution
"Ukrainian State University of Chemical Technology"

ЗМІСТ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ ЯК ВАЖЛИВОЇ ПІДСИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА МАКРО- ТА МЕЗОРІВНЯХ

CONTENTS OF INFORMATION AND PSYCHOLOGICAL SECURITY AS AN IMPORTANT SUBSYSTEM OF INFORMATION SECURITY AT MACRO- AND MESOLEVEL

Характерною рисою сучасного суспільства стало проникнення інформаційних технологій у різні сфери людської діяльності: науку, економіку, політику та управління. Інформаційна безпека досягається лише за системного підходу, розумного поєднання законодавчих, організаційних та програмно-технічних заходів. Метою роботи є розгляд змісту підсистеми інформаційно-психологічної безпеки та виділення особливостей інформаційно-психологічного впливу на особистості, соціальні групи та суспільство на макро- та мезорівнях. У роботі запропоновано розглядати інформаційну сферу з погляду двох основних складників: інформаційно-технічної сфери та інформаційно-психологічної сфери. Процеси реформування, що відбуваються нині в економіці, соціальному та духовному житті України та її регіонів, виявляються суттєво залежними від різного роду інформаційно-психологічних впливів. Авторами запропоновано виділити основні групи об'єктів захисту як практичне вирішення завдань забезпечення інформаційно-психологічної безпеки особистості, суспільства, регіону та держави в сучасних умовах, а також суб'єктів інформаційно-психологічного впливу. У роботі зазначено базові засоби та методи інформаційно-психологічного впливу та виділено їхні особливості, які становлять зміст інформаційно-психологічної безпеки.

Ключові слова: інформаційна безпека регіону, інформатизація, інформаційно-технічна безпека, інформаційно-психологічна безпека, інтелектуальна безпека, інформаційна сфера.

Характерной чертой современного общества стало проникновение информационных технологий в различные сферы человеческой деятельности: науку, экономику, политику и управление. Информационная безопасность достигается лишь при системном подходе, разумном сочетании законодательных, организационных и программно-технических мероприятий. Целью работы является рассмотрение содержания подсистемы информационно-психологической безопасности и выделение особенностей информационно-психологического влияния на личности, социальные группы и общество на макро- и мезоуровне. В работе предложено рассматривать инфор-

мационную сферу с точки зрения двух основных составляющих: информационно-технической сферы и информационно-психологической сферы. Процессы реформирования, происходящие в настоящее время в экономике, социальной и духовной жизни Украины и ее регионов, оказываются существенно зависимыми от разного рода информационно-психологических воздействий. В работе отмечены базовые средства и методы информационно-психологического воздействия и выделены их особенности, которые составляют содержание информационно-психологической безопасности.

Ключевые слова: информационная безопасность региона, информатизация, информационно-техническая безопасность, информационно-психологическая безопасность, интеллектуальная безопасность, информационная сфера.

Penetration of information technology into various fields of human activity: science, economics, politics and management has become a characteristic feature of modern society. Due to wide informatization of the main aspects of life activity, information sphere has become an important part of the public life of Ukraine and its regions, it largely determining the direction of socio-political and economic development of the state. It should be noted that information security is achieved only through a systems approach, a reasonable combination of legislative, organizational and program-technical measures. The purpose of the work is to consider the content of information and psychological security subsystem and to show the peculiarities of information and psychological impact on individuals, social groups and society at macro- and mesolevel. The paper proposes to consider information sphere within the limits of macro-, meso- and microlevels from the point of view of two main components: information-technical as well as information-psychological sphere. Security functions in the region's information security system are considered. Information and psychological security at regional level is the protection of the emotional and psychological environment of the region from the influence of negative information including false (untrue), distorted and tendentious one. The authors suggest to identify the main groups of objects of protection as a practical solution to the tasks for ensuring information and psychological security of the individual, society, region and state in modern conditions, as well as subjects of information and psychological influence. The basic means and methods of informational and psychological influence are stated in the work. The peculiarities constituting the content of information and psychological security are marked out. The objects of manipulation may be economic and social subjects of different levels of community – from individual to society of the region (territory) or to the society of the country as a whole. In order to prevent threats to information and psychological security at macro- and mesolevel it is necessary to adopt legislative acts on protecting individuals, special groups of society from negative information and psychological influences at the state level, as well as to develop and start implementing a program for using psychotechnology in the interests (first of all social-economic interests) of the state of Ukraine and its regions.

Key words: information security of the region, informatization, information and technical security, information and psychological security, intellectual security, information sphere.

Постановка проблеми. Одним зі складників економічної безпеки є інформаційна безпека. Інформаційна безпека досягається лише за системного підходу – розумному поєднанні законодавчих, організаційних та програмно-технічних заходів. Стрімкий розвиток ринку інформаційних послуг на сучасному етапі на макро-, мезо- та мікрорівнях супроводжується появою великої кількості загроз його якісному функціонуванню. Слід відзначити, що інформаційною безпекою нині називають те, що в 60–70-х роках XX ст. іменувалося комп'ютерною безпекою, а з початку 80-х років – безпекою даних.

Якщо розглядати інформаційну безпеку в міжнародному аспекті, то вона трактується, передусім, виходячи з характеру загроз. Традиційно виділяється «тріада загроз» міжнародній інформаційній безпеці: використання інформаційних комп'ютерних технологій у військово-політичних, терористичних та злочинних цілях, тобто використання IT-технологій у міждержавних конфліктах.

Значущість національних інтересів України у сфері забезпечення інформаційної безпеки та управління мережею Інтернет особливо підкреслює той факт, що вони згадуються у цілому переліку офіційних документів. У цьому контексті термін «інформаційна безпека» трактується як стан захищеності національних інтересів в інформаційному середовищі, які визначаються сукупністю збалансованих інтересів особистості, суспільства та держави. Інформаційна безпека в умовах макро-, мезо- та мікрорівнів – це комплекс організаційно-технічних заходів, які забезпечують цілісність даних та конфіденційність інформації у поєднанні з її доступністю для всіх авторизованих користувачів. Цілі, досягнення яких гарантує інформаційна безпека, можна сформулювати так: конфіденційність критичної інформації; цілісність інформації й зв'язаних із нею процесів створення,

введення, обробки та виведення інформації; доступність інформації у разі необхідності; облік інформації.

У загальному плані ринок безпеки інформаційних систем можливо умовно розділити на два ідеологічно не пов'язані між собою напрями. *Перший напрям* має своєю метою інформаційний захист мереж, тобто захист інформації, яка циркулює всередині інформаційних мереж. Сьогодні це найбільш затребуваний, а тому й досить добре розвинутий напрям. Сюди слід віднести різноманітні антивірусні програми, міжмережеві фільтри, захисні протоколи, цифрові підписи та інші засоби захисту мережі. *Другий напрям,* який достатньо стрімко розвивається в останній час, пов'язаний із безпосереднім захистом об'єктів мережі. Цей напрям представляють переважно механічні пристрої, які попереджають доступ до апаратної частини, тобто до серверів, персональних комп'ютерів тощо.

Ймовірніше за все, у майбутньому ми будемо свідками інтеграції цих двох напрямів, що є єдиним кроком на шляху до підвищення рівня захисту інформації в межах макро-, мезо- та мікрорівнів. У результаті такої інтеграції зможе з'явитися якась універсальна система безпеки, а у адміністратора безпеки буде єдине робоче місце, з якого він зможе контролювати порядок обробки даних та цілісність об'єктів.

У повсякденній практичній діяльності у зв'язку з масовою інформатизацією сучасного суспільства все більшої актуальності набуває знання правових основ та морально-етичних норм використання засобів нових інформаційних технологій. Слід відзначити, що інформаційна безпека досягається лише за системного підходу, розумного поєднання законодавчих, організаційних та програмно-технічних заходів. Велика кількість катастроф у глобальній економіці – нагадування про серйозний прорахунок: усе більше довіряючи машинам, люди постійно забувають, де проходять межі і свідомого контролю, і моральної відповідальності та інформаційно-психологічної стійкості.

Дана робота – узагальнення теоретико-експериментальних досліджень авторів. Вона присвячена маловивченій проблемі аналізу непрямого (побічного, багатократно опосередкованого) впливу інформаційних технологій в умовах макро-, мезо та мікрорівней, який призводить до зміни традиційних (неінформатизованих) форм діяльності. Слід виділити перелік основних принципів впливів такого роду:

1. Принцип розповсюдження перетворень: перетворена під впливом інформаційних технологій діяльність сама стає джерелом наступних перетворень інших видів діяльності.

2. Принцип зворотних дій: зміна конкретного виду інформаційної діяльності може призвести до зміни неінформатизованої (традиційної) форми цієї ж діяльності.

3. Принцип генералізації перетворень: психологічні наслідки інформатизації можуть зачіпати не тільки окремі психічні процеси, але й усю особистість у цілому.

4. Принцип інтерференції перетворень: одні психологічні наслідки інформатизації накладаються на інші, що може призвести до гіперболізації та нейтралізації процесів.

У даній роботі передбачається узагальнене представлення деяких умов реалізації вказаних принципів, психологічних механізмів та наслідків інформатизації в умовах забезпечення економічної безпеки на макро-, мезо- та макрорівнях, а також викладення основних положень інформаційно-психологічної безпеки, яка є підсистемою системи інформаційної безпеки у сфері забезпечення економічної безпеки на національному та регіональному рівнях.

Аналіз останніх досліджень і публікацій. Проблема економічної та інформаційної безпеки в умовах трансформації національної та регіональної економіки розглянута в роботах В.В. Піменова, П.К. Шафранського [1], А.М. Гуменюка [2], А.П. Курило, С.Л. Зефирова та В.Б. Голованова [3], В.Г. Кулакова [4], А.Г. Светлакова та І.М. Глобіна [5], А.О. Малюк та О.Ю. Полянської [6], В.Н. Усцилемова [7], Г.Г. Почепцова [8]. До досліджень, які відносяться до методології формування системи інформаційної безпеки на національному та регіональному рівнях, слід віднести роботи В.В. Аратюнова [9], Є.С. Кадцини [10], Л.Г. Матвєєвої [11], С.В. Любавіної [12], а також Ф. Уебстера [13]. Проблеми формування та функціонування підсистеми інформаційної безпеки – інформаційно-психологічної безпеки досліджуються в роботах: В.А. Баришполеца [14], О.М. Федорової [15], А.Ю. Нашинець-Наумової [16], В.М. Юрченко та І.В. Юрченко, Є.В. Савва та І.А. Герасимова [17], а також Г. Хакена [18], Ю. Брумштейна, А. Підгорного [19], С.М. Ненашева [20], В.Я. Асановича та Г.Г. Маньшина [21], Ю.Д. Бабаєвої, А.Є. Войскунского [22], А.В. Манойло, А.І. Петренка, Д.Б. Фролова [23], І.В. Юрченко [24].

Формулювання цілей статті (постановка завдання). Метою роботи є розгляд змісту підсистеми інформаційно-психологічної безпеки та виділення особливостей інформаційно-психологічного впливу на особистості, соціальні групи та суспільство на макро- та мезорівнях.

Виклад основного матеріалу дослідження. Адекватне розуміння проблеми безпеки передбачає усвідомлення системної природи даного явища і, отже, необхідності системного підходу

до його вивчення. Такий підхід ґрунтується на розгляді характеру взаємодії внутрішніх компонентів та елементів системи та зовнішнього середовища, яке здійснює безпосередній вплив, а інколи й жорсткий соціальний тиск на різноманітні сегменти суспільства, які повинні забезпечувати безпеку громадян, соціальних груп, населення держави та її регіонів у цілому. Під небезпекою розуміється об'єктивно існуюча можливість деструктивного впливу на систему (економічну, соціальну, політичну, екологічну та ін.) із боку зовнішніх сил, у результаті якого може бути завдана суттєва шкода. Небезпеки можуть являти собою як цілеспрямовані результати навмисних дій із чийогось боку, так і природне походження, а отже, ненавмисний характер, тоді як загроза несе безпосередню небезпеку, джерело якої може бути встановлено більш-менш точно, тобто загроза потребує швидкого реагування з боку тих, проти кого вона направлена. Ризики – це ті ймовірно можливі небезпеки, щодо яких зроблено заходи для підстраховування або профілактичні дії. Частіше термін «ризик» трактується як імовірність збитку.

Однак проблема полягає у тому, що неможливо вивести абсолютно об'єктивні та незаперечні критерії визначення потенційного збитку. І наостанок, вразливість – один з індикаторів стану безпеки соціально-економічної системи, території (регіону), яка свідчить про її потенціальну незахищеність перед лицем зовнішніх викликів. Поняття «безпека» в широкому плані може трактуватися як стійкість системи, території або соціально-економічної структури відносно кризисних змін та впливу чинників, які формують ризики кризи. Масштаби кризових процесів виявляють тенденцію їх прогресуючого зростання, який зумовлений ускладненням технологічних, фінансових, інформаційних, соціально-економічних та політичних взаємозв'язків. Вони визначають усі важко передбачувані нові комбінації параметрів загроз та ризиків безпеки як на загальнодержавному, так і на регіональному рівні [3, с. 12].

Система критеріїв та індикаторів економічної безпеки регіону визначається як порогові показники, вихід за межі яких означає появу реальних загроз конкретному регіону. Розроблення індикаторів – складна методологічна проблема. Окрім традиційно використовуваних кількісних макроекономічних та мезоекономічних показників (ВВП, ВРП, національного та регіонального доходу та ін.), у соціально-економічній діагностиці необхідні індикатори на основі «показників тривоги», порівняння яких із фактичними параметрами за видами економічної безпеки (держави, регіону, суб'єктів господарювання, громадян) дає змогу своєчасно побачити перевищення граничних значень. Вони слугують сигналами до своєчасного реагування з боку державних або регіональних структур. Тому розроблення механізмів забезпечення регіональної безпеки (у т. ч. за системами соціальної, інформаційної, екологічної, демографічної, фінансової, інноваційної та іншої безпеки) повинна мати перманентний характер.

У межах забезпечення економічної безпеки регіону проблема забезпечення інформаційної, інформаційно-технічної, інформаційно-психологічної та інтелектуальної безпеки – найважливіша умова їх успішного соціально-економічного функціонування та розвитку. На жаль, в існуючих дослідженнях у сфері економічної безпеки регіону та інформаційної безпеки регіонів по відношенню до регіонів у цілому питання інформаційної, інформаційно-психологічної та інтелектуальної безпеки відображені слабо, при цьому тематика інформаційно-психологічної безпеки в ув'язці інформаційної безпеки та інтелектуальної безпеки не вивчена. У даному дослідженні автори розглядають основні положення інформаційно-психологічної безпеки на рівні регіону за складником «громадяни території» [20, с. 67–68].

У зв'язку з широкою інформатизацією основних боків життєдіяльності **інформаційна сфера** стала важливою частиною суспільного життя України та її регіонів, багато в чому визначає напрям соціально-політичного та економічного розвитку держави. **Інформаційну сферу** – сферу діяльності суб'єктів суспільного життя, пов'язану зі створенням, збором, перетворенням, зберіганням, розповсюдженням та дослідженням інформації в межах макро-, мезо- та мікрорівнів, можна розділити на дві основні складові частини: ***інформаційно-технічну сферу*** та ***інформаційно-психологічну сферу***. Інформаційно-технічна сфера пов'язана з інформаційним забезпеченням усіх боків життєдіяльності особистості (громадян держави, регіону, території, суспільства, держави) за допомогою використання інформаційних та телекомунікаційних систем. Інформаційно-психологічна сфера утворюється сукупністю людей та інформації, якою вони обмінюються й яку сприймають, суспільних відносин, які виникають у зв'язку з інформаційним обміном та інформаційно-психологічним впливом на людину. На рис. 1 представлено авторське розуміння інформаційної безпеки регіону.

Інформаційно-психологічна безпека на рівні регіону – це передусім захищеність емоційно-психологічного середовища регіону від впливу негативної інформації, включаючи помилкову

(недостовірну), спотворену та тенденційну. При цьому інтелектуальну безпеку регіону визначимо як захищеність інтелектуальних ресурсів юридичних та фізичних осіб у регіоні від знищення, деградації, втрати, зниження ефективності використання, погіршення якісних характеристик, порушення можливостей взаємодії для інтелектуальних ресурсів юридичних та фізичних осіб регіону. Відзначимо, що безпека для інтелектуальної безпеки та ефективність їх використання залежать від інформаційної безпеки регіону.

У фундаментальному дослідженні В.А. Баришполеца представлено авторське визначення інформаційно-психологічної безпеки на національному рівні: «Інформаційно-психологічна безпека держави – це захищеність громадян, окремих груп та соціальних верств, масових об'єднань людей та населення країни у цілому від негативного інформаційно-психологічного впливу» [14, с. 63].

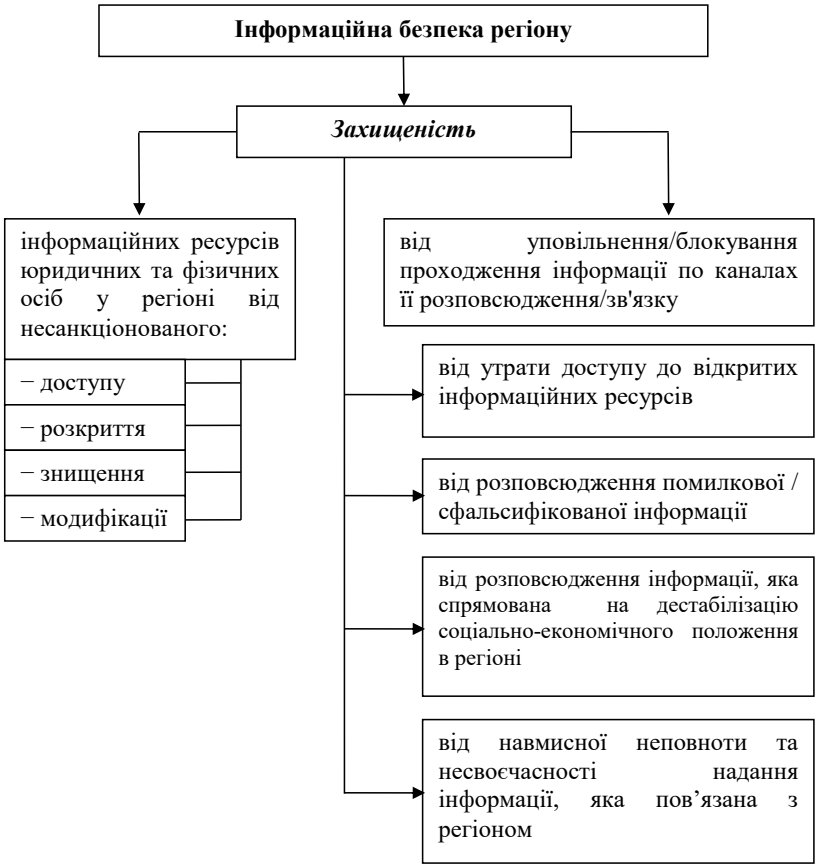

Рис. 1. Функції захищеності в системі інформаційної безпеки регіону

Процеси реформування, що відбуваються сьогодні в економіці, соціальному та духовному житті України та її регіонів, виявляються суттєво залежними від різного роду ***інформаційно-психологічних впливів***. Ці впливи в загальних рисах кваліфікуються як негативні, якщо викликають психоемоційну та соціально-психологічну напруженість у різних соціальних групах регіонів й у цілому в українському суспільстві (спотворення моральних критеріїв та норм, погіршення здоров'я на генетичному рівні, морально-політична дезорієнтація і, як наслідок, неадекватна поведінка окремих осіб, груп та мас людей і т. ін.). Їх основні наслідки – глибока трансформація індивідуальної, групової, масової та суспільної свідомості, зміна морально-політичного та соціально-психологічного клімату в суспільстві. Негативний інформаційно-психологічний вплив якоюсь мірою корелюється також із маніпулятивними прийомами, які спрямовані на програмування думок і прагнень мас, їхніх настроїв і навіть психічного стану людей для забезпечення такої їхньої поведінки, яка потрібна тим, хто володіє засобами маніпуляції [14, с. 17].

Виходячи з вище викладеного, поняття **«негативний інформаційно-психологічний вплив»**, яке є визначальним для інформаційно-психологічної безпеки, може бути сформульовано так: *інформаційно-психологічний вплив на людину (особистість), на групову, масову та суспільну свідомість із метою явного або скритого спонукання індивідуальних або соціально-економічних суб'єктів до дій у збиток власним економічним інтересам в інтересах окремих осіб, груп або організацій, які здійснюють цей вплив.*

Сфера організації інформаційно-психологічного впливу на психіку людини, групову, масову та суспільну свідомість у межах держави, регіону та території включає у себе об'єкти інформаційно-психологічного впливу, суб'єктів, які впливають на ці об'єкти, комунікацію між суб'єктами та об'єктами інформаційно-психологічного впливу, а також засоби та методи інформаційно-психологічного впливу.

Слід відзначити, що головними мішенями інформаційно-психологічного впливу виступають індивідуальні, групові, масові та суспільні свідомості. Виходячи із цього, об'єктами інформаційно-психологічного впливу є:

– людина (особистість – її психіка, свідомість, організм);

– різні громадські організації;

– соціальні групи людей;

– населення регіонів та країни у цілому.

Як відзначають дослідники [14–16; 18–21] людина, її повсякденне життя все більше залежать від масової комунікації, яка утворює свого роду «другу суб'єктивну реальність», влив якої не менш значний, аніж вплив об'єктивної реальності [25, с. 41]. Людина як об'єкт інформаційно-психологічного впливу може розглядатися, по-перше, як громадянин (особистість) та, по-друге, як індивід. Як громадянин (держави або регіону) людина є суб'єктом економіко-політичного життя, який володіє певним світоглядом, більш-менш правосвідомістю та менталітетом, духовними ідеалами та ціннісними установками. Основна суть інформаційно-психологічного впливу у цьому разі зводиться до того, щоб поведінка громадянина (держави, регіону та його території) була адекватною тим чи іншим суспільним та економічним інтересам. Людина як особистість та активний економіко-соціальний суб'єкт може бути піддана інформаційно-психологічному впливу, який трансформується через її поведінку, дії (або бездіяльність), надає дисфункційний вплив на різні соціальні структури країни, регіону.

Держава через свої інститути (освіти, права, культури, армії, спорту та ін.) формує члена соціуму, спрямовує та корегує вектор розвитку «індивідуальної людини». Своєю чергою, «індивідуальна людина» творить закони та права, управляє державою та її структурами (регіонами, територіями), формуючи в необхідному плані розвиток «людини колективної». Цей взаємно корельований процес реалізується за допомогою економіко-соціальної та індивідуальної систем трансформації.

На рис. 2 представлено виділення основних груп об'єктів захисту як практичне вирішення завдань забезпечення інформаційно-психологічної безпеки особистості, суспільства, регіону та держави в сучасних умовах.

Перераховані на рис. 2 об'єкти є в рамках держави, регіонів, території носіями індивідуальної, групової, масової та громадської свідомості та підлягають захисту від негативного інформаційно-психологічного впливу.

Суб'єкт інформаційно-психологічного впливу (комунікатор) – це джерело інформації в межах країни та її регіонів, який володіє технологіями управління інформаційними процесами та мані-

Рис. 2. Основні об'єкти (групи захисту) забезпечення інформаційно-психологічної безпеки

пулювання інформацією (у т. ч. загрозливою економічним інтересам різних груп країни та її регіонів), а також управління поведінкою соціальних систем (об'єктів) – людей, соціальних груп, суспільства.

Комунікатор порівняно з об'єктом впливу (аудиторією) володіє явною перевагою, яка полягає у його комплексності, системності, масштабності та цілеспрямованості. Суб'єктами інформаційно-психологічного впливу на окрему людину, групу людей, населення регіонів та країни у цілому можуть бути суб'єкти, представлені на рис. 3.

Рис. 3. Суб'єкти інформаційно-психологічного впливу

Під комунікацією (лат. communicatio – роблю загальним, зв'язую, спілкуюся) у маркетингу соціально-економічної психології розуміється спілкування, передача інформації, інформаційний вплив людей, бізнес-структур у процесі їхньої пізнавально-трудової діяльності, а також між людиною та економіко-техніко-технологічною системою. Найчастіше вона пов'язана з опосередкованим спілкуванням за допомогою друкованих засобів та технічних пристроїв. Як процес обміну інформацією комунікація включає такі елементи: джерело (комунікатор) – повідомлення – канал комунікації – одержувач (реципієнт), а також кодування та декодування інформації. Передача інформації в межах країни та її регіонів здійснюється за допомогою каналів комунікації, які являють собою спеціально сформоване середовище або спосіб розповсюдження інформації від джерела інформації до одержувача [13, с. 217].

Слід підкреслити, що всі канали комунікації інформаційно-психологічного впливу володіють різними характеристиками, мають і переваги, і недоліки, тому не можна вибирати єдиний канал та обмежуватися ним. Найбільш ефективним за інформаційно-психологічного впливу на індивідуальні, групові, масові та громадянські свідомості є багатоканальний вплив, коли кожний із каналів виконує свою функцію.

Щоб створювати засоби та методи захисту від будь-якого інформаційно-психологічного впливу, необхідно досконально знати спеціальні засоби та методи, які використовуються для цього впливу. З погляду фізичної сутності, принципів та механізмів впливу засоби та методи інформаційно-психологічного впливу можуть бути класифіковані так: переконання та сугестивні методи, інформаційно-техногенні методи, психотропні методи, феноменологічні методи, комбіновані методи.

Базові засоби та методи інформаційно-психологічного впливу (рис. 4):

1) переконання: метод відкритого вербального (словесного) інформаційно-психологічного впливу на свідомість індивіда або групи людей, основу якого становить система ясних, чітко сформульованих доводів, які побудовані за законами формальної логіки;

2) феноменологічні засоби: взаємодія живих істот із розвинутою рецепцією (чутливістю до сигналів/загроз навколишнього світу), пов'язана з прийомом та передачею сигналів/інформації від однієї системи до іншої, тобто інформаційна взаємодія;

3) комбіновані засоби: під комбінованими засобами та методами інформаційно-психологічного впливу розуміється практично одночасне застосування двох та більше засобів (методів) такого впливу; наприклад комплексне аудіо- та відеосугестії (зорової усвідомлюваної інформації та неусвідомлюване акустичне навіювання);

4) техногенні засоби та методи: до інформаційно-техногенних засобів та методів інформаційно-психологічного впливу належать інформаційні та технічні психотехнології з використанням обчислювальної, акустичних систем з «інтелектуальним сигналом»; вплив по вектору «техніка – людина» (інформаційно-психологічний вплив за допомогою засобів масової інформації, Інтернет та комп'ютерні відеоігри, вплив хвильових процесів, біорезонансна стимуляція);

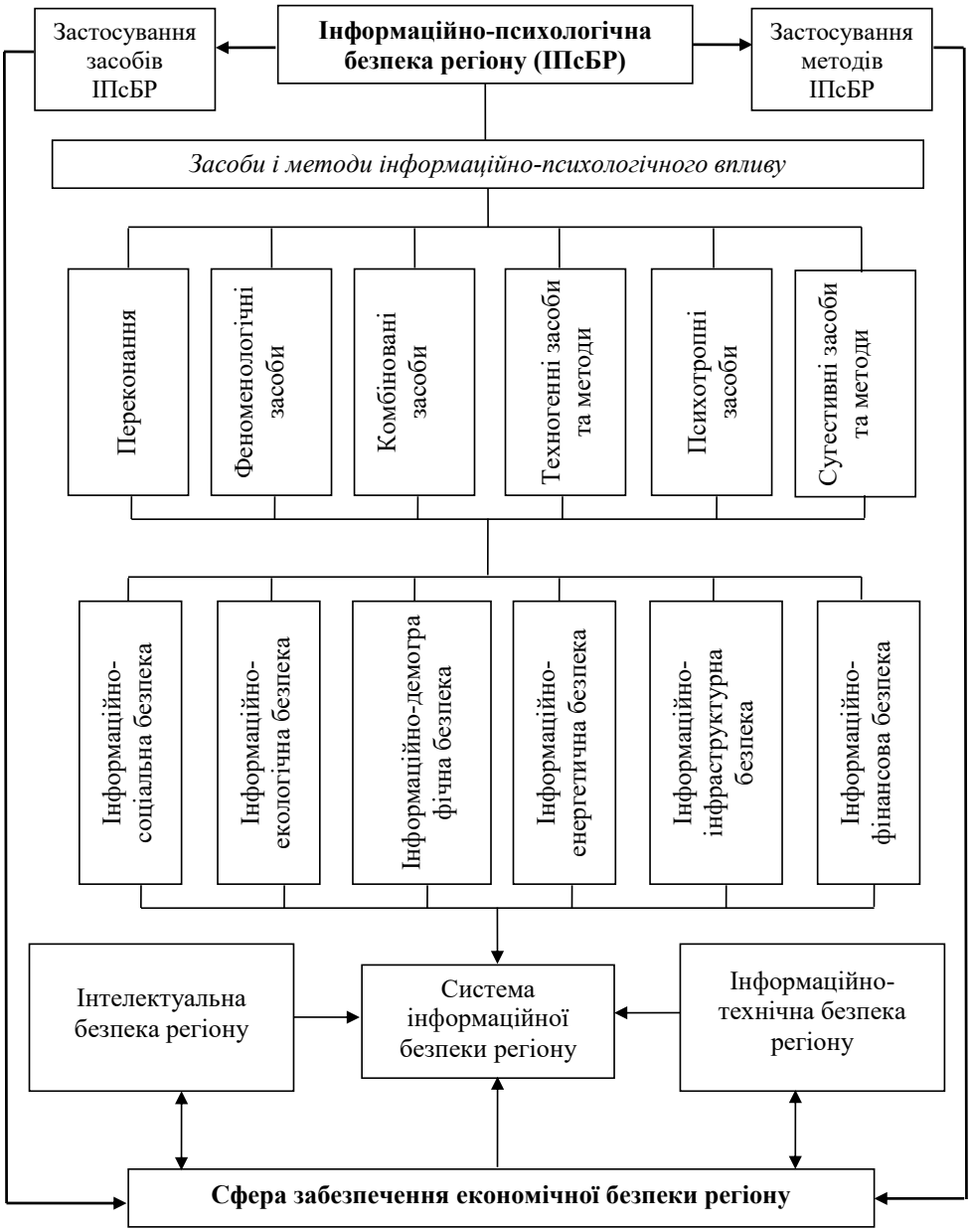

Рис. 4. Зміст інформаційно-психологічної безпеки (засоби і методи інформаційно-психологічного впливу)

5) психотропні засоби: до психотропних засобів інформаційно-психологічного впливу належить група біологічно активних речовин, які впливають переважно на психічні функції особистості, а також здатні переводити її в змінений стан свідомості; спостерігається клінічний ефект психолептики під час сприйняття інформації;

6) сугестивні засоби та методи: сугестія (навіювання) – це процес неаргументованого інформаційно-психологічного впливу на свідомість індивіда або групи, який пов'язаний зі зниженням критичності під час сприйняття та реалізації ним змісту інформації, що повідомляється, пропаганда, неусвідомлювана акустична інформація, неусвідомлювана зорова інформація, гіпнотичні методи, метод нейролінгвістичного програмування, тренінг інформаційно-психологічного впливу (цілеспрямований).

Коли йдеться про маніпулювання свідомістю, то мається на увазі переносне значення цього слова – спритне поводження з людьми як з об'єктами або обробка їх у своїх інтересах та приховане управління ними. Маніпуляція свідомістю під час використання методів (технологій) інформаційно-психологічного впливу стосовно впливу на людину чи на підприємницьку діяльність – це специфічний вид скритого інформаційно-психологічного впливу, який спрямований на програмування ідей, думок, мотивів, життєвих чи бізнес-установок,

стереотипів, прагнень, настроїв і навіть психічного стану людей із метою такої їхньої поведінки, яка потрібна тим, хто володіє засобами маніпуляції [14, с. 94–95].

Це досягається впровадженням маніпуляційної інформації на тлі посланих відкрито відволікаючих повідомлень прямо у підсвідомість, минаючи етап критичного сприйняття її свідомістю людини. Іншими словами, маніпуляція свідомості – це вид скритого інформаційно-психологічного впливу, метою якого не повинна бути усвідомлена об'єктом маніпуляція. Головна мета маніпуляції свідомістю в межах забезпечення інформаційної безпеки в умовах країни або регіону, – щоб викриття самого факту спроби маніпуляції не призвело до з'ясування подальших намірів.

Маніпулятивний інформаційно-психологічний вплив сприймається, як правило, зі знаком мінус. Однак слід обмовитися, що бувають ситуації, коли в силу складних обставин маніпулятивний інформаційно-психологічний вплив може носити позитивний характер. Об'єктами маніпуляції свідомістю можуть виступати економічні та соціальні суб'єкти різного рівня спільності – від індивіда до суспільства регіону (території) або до суспільства країни у цілому. Інформаційно-психологічний вплив із метою викликати певні емоційні стани є складовою частиною маніпуляції свідомості. Емоційні стани людей, груп суттєво впливають на сприйняття різного роду інформаційних повідомлень. Вони можуть полегшувати або, навпаки, ускладнювати їх сприйняття.

Спеціалісти виділяють у процесі інформаційно-психологічного впливу три рівня маніпуляції свідомістю:

– посилення існуючих у свідомості людей необхідних маніпулятору ідей, життєвих установок, мотивів, цінностей, норм;

– мала (приватна) зміна поглядів (у т. ч. емоційного та практичного відношення) на ту чи іншу подію, факт, процес;

– корінна, кардинальна зміна життєвих установок шляхом повідомлення об'єкту сенсаційних, драматичних, надзвичайно важливих для нього відомостей.

При цьому необхідно відзначити, що в сучасних умовах в інформаційно-комунікаційних процесах на макро-, мезо- та мікрорівнях використовуються не просто окремі прийоми, а спеціальні маніпулятивні технології. Знання маніпулятивних технологій та прийомів інформаційно-психологічного впливу на людину, соціальну групу, певну територію регіону необхідно для формування індивідуального та групового інформаційно-психологічного захисту у сфері забезпечення економічної безпеки як на мезорівні, так і на макрорівні.

Забезпечення інформаційно-психологічної безпеки – це запобігання або парирування небезпек та загроз, які пов'язані з інформаційно-психологічним впливом на індивідуальну, групову, масову та громадянську свідомість, а також ліквідація наслідків цілеспрямованого негативного інформаційно-психологічного впливу. Виконання вказаних функцій повинно здійснюватися системою забезпечення інформаційно-психологічної безпеки на мікро- та мезорівнях, а також у цілому на макрорівні, тобто безпеки держави.

Висновки з даного дослідження. Усвідомлення суворої реальності існування інформаційно-психологічного впливу викликає необхідність уважного розгляду проблеми забезпечення захисту індивідуальної, групової, масової та громадської свідомості від подібних впливів, які мають негативний (деструктивний) характер.

Можливість деструктивного інформаційно-психологічного впливу на людину з метою модернізації його психіки може призвести до катастрофічних наслідків для держави та її регіонів, якщо не прийняти завчасно заходи щодо нейтралізації такого впливу. З метою парирування загроз інформаційно-психологічної безпеки на макро- та мезорівнях, необхідно на державному рівні прийняти законодавчі акти щодо захисту особистості, спеціальних груп суспільства від негативних інформаційно-психологічних впливів, а також розробити та приступити до реалізації програми використання психотехнологій в інтересах, насамперед, соціально-економічних інтересів, держави Україна та її регіонів.

Список використаних джерел:

1. Пименов В.В., Шафранский П.К. Экономическая и информационная безопасность в условиях трансформации: инструменты и механизмы по их нейтрализации. *Экономическая безопасность и качество*. 2018. № 1(30). С. 25–30.
2. Гуменюк А.М. Безпека структурно-інституціональної трансформації економіки регіону: теоретичні основи та приклади аспекти : монографія. Київ : НІСД, 2014. 468 с.
3. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности. Москва : БДЦ-пресс, 2006. 304 с.
4. Кулаков В.Г. Региональная система информационной безопасности: угрозы, управление и обеспечение : дис. … доктора техн. наук : 05.13.19. Воронеж, 2005. 332 с.

5. Светлаков А.Г., Глобина И.М. Влияние информационного пространства на экономическую безопасность региона. *Экономика региона*. 2018. Т. 14. Вып. 2. С. 474–484.
6. Малюк А.А., Полянская О.Ю. Зарубежный опыт формирования в обществе культуры информационной безопасности. *Безопасность информационных технологий.* 2016. № 4. С. 25–37.
7. Усцилемов В.Н. Совершенствование подсистемы информационной безопасности на основе интеллектуальных технологий. *Прикладная информатика*. 2016. Т. 11. № 3(63). С. 31–38.
8. Почепцов Г.Г. Информационно-психологическая война. Москва : СИНТЕГ, 2002. 180 с.
9. Аратюнов В.В. Современные проблемы и задачи обеспечения информационной безопасности. *Вестник МФЮУ*. 2016. № 2. С. 213–222.
10. Кадцына Е.С. Концептуальная модель оценки и оптимизации развития процесса региональной информатизации. *Вестник РЭА им. Г.В. Плеханова*. 2018. № 6(102). С. 185–198.
11. Матвеева Л.Г., Никитаева А.Ю., Чернова О.А. Информация как стратегический ресурс регионального развития: институционально-технологические аспекты. *TERRA Economicus*. 2018. Т. 16. № 1. С. 134–145.
12. Любавина С.В. Оптимизация информационной системы процесса управления регионом. *Региональные проблемы преобразования экономики*. 2018. № 3. С. 34–42.
13. Уэбстер Ф. Теории информационного общества / пер. с англ. М.В. Арапова, Н.В. Малыхиной ; под ред. Е.Л. Вартановой. Москва : Аспект-пресс, 2004. 400 с.
14. Баришполец В.А. Информационно-психологическая безопасность: основные положения. *Труды РЭНСИТ. Серия «Информационные технологии»*. 2013. Т. 5. № 2. С. 62–104.
15. Федорова О.Н. Информационно-психологическая безопасность личности в информационном обществе. *Вестник ДГТУ*. 2011. № 2(7). С. 21–34.
16. Нашинець-Наумова А.Н. Інформаційна агресія як основний компонент інформаційної війни. *Інформаційне право*. 2015. № 6. С. 66–69.
17. К построению модели информационной безопасности полиэтничного региона (на материалах Юга России) / В.М. Юрченко и др. *Человек. Сообщество. Управление*. 2010. № 4. С. 4–15.
18. Хакен Г. Информация и самоорганизация. Макроскопический подход к сложным явлениям. Москва : Мир, 1991. 240 с.
19. Брумштейн Ю.М., Подгорный А.Н. Комплексный анализ факторов информационной и интеллектуальной безопасности регионов. *Информационная безопасность регионов*. 2011. № 1(8). С. 8–14.
20. Ненашев С.М. Информационно-технологическая и информационно-психологическая безопасность пользователей социальных сетей. *Вопросы кибербезопасности*. 2016. № 5(18). С. 65–72.
21. Асанович В.Я., Маньшин Г.Г. Информационная безопасность и прогноз информационного воздействия. Минск : Амалфея, 2006. 320 с.
22. Бабаева Ю.Д., Войскунский А.Е. Психологические последствия информатизации. *Психологический журнал*. 1998. Т. 19. № 1. С. 89–100.
23. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны : монография. Москва : Горячая линия – Телеком, 2009. 320 с.
24. Юрченко И.В. Региональная безопасность как предмет конфликтологического анализа (апология методологического плюрализма). *Полис. Политические исследования.* 2007. № 6. С. 122–132. DOI : https://doi.org/10.17976/jpps/2007.06.11.
25. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. Москва : РАГС, 1998. 125 с.

References:

1. Pimenov V. V., Shafranskij P. K. (2018) Jekonomicheskaja i informacionnaja bezopasnost' v uslovijah transformacii: instrumenty i mehanizmy po ih nejtralizacii [Economic and information security in the conditions of transformation: tools and mechanisms for their neutralization]. *Economic safety and quality*, 1(30), 25-30. (in Russian)
2. Gumenyuk A. M. (2014) Bezpeka strukturno-insty`tucional`noyi transformaciyi ekonomiky` regionu: teorety`chni osnovy` ta pry`klady` aspekty` : monografiya [Security of structural and institutional transformation of the region's economy: theoretical foundations and examples aspects: monograph]. Kiev: NISD. (in Ukrainian)
3. Kurilo A. P., Zefirov S. L., Golovanov V. B. (2006) Audit informacionnoj bezopasnosti [Information Security Audit]. Moscow: publishing group «BDC-press». (in Russian)
4. Kulakov V. G. (2005). *Regional information security system: threats, management and security* [Regional information security system: threats, management and support] (Doctor's thesis), Voronezh. (in Russian)
5. Svetlakov A. G., Globina I. M. (2018) Vlijanie informacionnogo prostranstva na jekonomicheskuju bezopasnost' regiona [The influence of the information space on the economic security of the region]. *The economy of the region*, 14 (2), 474-484. (in Russian)

6. Maljuk A. A., Poljanskaja O. Ju. (2016) Zarubezhnyj opyt formirovanija v obshhestve kul'tury informacionnoj bezopasnosti [Foreign experience in the formation of a culture of information security in society[. *Information Technology Security*, 4, 25-37. (in Russian)
7. Uscilemov V. N. (2016) Sovershenstvovanie podsistemy informacionnoj bezopasnosti na osnove intellektual'nyh tehnologij [Improving the information security subsystem based on intelligent technologies]. *Applied Informatics*, 3(63), 31-38. (in Russian)
8. Pochepcov G. G. (2002) Informacionno-psihologicheskaja vojna [Information and psychological warfare]. Moscow: SINTEG. (in Russian)
9. Aratjunov V. V. (2016) Sovremennye problemy i zadachi obespechenija informacionnoj bezopasnosti [Modern problems and tasks of ensuring information security]. *Bulletin of the IFUU*, 2. 213-222. (in Russian)
10. Kadcyna E. S. (2018) Konceptual'naja model' ocenki i optimizacii razvitija processa regional'noj informatizacii [A conceptual model for assessing and optimizing the development of the regional informatization process]. *Herald REA them. G.V. Plekhanov*, 6(102), 185-198. (in Russian)
11. Matveeva L. G., Nikitaeva A. Ju., Chernova O. A. Informacija kak strategicheskij resurs regional'nogo razvitija: institucional'no-tehnologicheskie aspekty [Information as a strategic resource for regional development: institutional and technological aspects]. *TERRA Economicus*, 16(1), 134-145. (in Russian)
12. Ljubavina S. V. (2018) Optimizacija informacionnoj sistemy processa upravlenija regionom [Optimization of the information system of the region management process]. *Regional problems of economic transformation,* 3, 34-42. (in Russian)
13. Ujebster F. (2004) Teorii informacionnogo obshhestva [Information Society Theories]. Moscow: Aspect Press. (in Russian)
14. Barishpolec V. A. (2013) Informacionno-psihologicheskaja bezopasnost': osnovnye polozhenija [Information and psychological security: key points]. *Proceedings of RANSIT. Series: Information Technology*, 5(2), 62-104. (in Russian)
15. Fedorova O. N. (2011) Informacionno-psihologicheskaja bezopasnost' lichnosti v informacionnom obshhestve [Information and psychological security of the individual in the information society]. *Herald of DSTU*, 2(7), 21-34. (in Russian)
16. Nashy`necz`-Naumova A. N. (2015) Informacijna agresiya yak osnovny`j komponent informacijnoyi vijny` [Information aggression as a major component of the information war]. *Information law*, 6, 66-69. (in Ukrainian)
17. Jurchenko V. M., Jurchenko I. V., Savva E. V., Gerasimov I. A. (2010) K postroenii modeli informacionnoj bezopasnosti polijetnichnogo regiona (na materialah Juga Rossii) [Toward a model of information security for a multi-ethnic region (based on materials from the South of Russia)]. *Person. Community.* Control, 4, 4-15. (in Russian)
18. Haken G. (1991) Informacija i samoorganizacija. Makroskopicheskij podhod k slozhnym javlenijam [Information and self-organization. A macroscopic approach to complex phenomena]. Moscow: World. (in Russian)
19. Brumshtejn Ju. M., Podgornyj A. N. (2011) Kompleksnyj analiz faktorov informacionnoj i intellektual'noj bezopasnosti regionov [Comprehensive analysis of factors of information and intellectual security of regions]. *Information security of the regions*, 1(8), 8-14. (in Russian)
20. Nenashev S. M. (2016) Informacionno-tehnologicheskaja i informacionno-psihologicheskaja bezopasnost' pol'zovatelej social'nyh setej [Information-technological and information-psychological security of users of social networks]. *Cybersecurity issues*, 5(18), 65-72. (in Russian)
21. Asanovich V. Ja., Man'shin G. G. (2006) Informacionnaja bezopasnost' i prognoz informacionnogo vozdejstvija [Information security and information impact forecast]. Minsk: Amalfey. (in Russian)
22. Babaeva Ju. D., Vojskunskij A. E. (1998) Psihologicheskie posledstvija informatizacii [The psychological consequences of informatization]. *Psychological Journal*, 19(1), 89-100. (in (in Russian)
23. . Manojlo A. V., Petrenko A. I., Frolov D. B. (2009) Gosudarstvennaja informacionnaja politika v uslovijah informacionno-psihologicheskoj vojny: monografija [State information policy in the context of the information-psychological war: a monograph]. Moscow: Hotline - Telecom. (in Russian)
24. Jurchenko I. V. (2007) Regional'naja bezopasnost' kak predmet konfliktologicheskogo analiza (apologija metodologicheskogo pljuralizma) [Regional security as a subject of conflict analysis (apology of methodological pluralism)]. *Policy. Political research*, 6, 122-132. DOI: https://doi.org/10.17976/jpps/2007.06.11(in Russian)
25. Grachev G. V. (1998) Informacionno-psihologicheskaja bezopasnost' lichnosti: sostojanie i vozmozhnosti psihologicheskoj zashhity [Information and psychological security of a person: state and possibilities of psychological defense] . Moscow: RAGS publishing house. (in Russian)