ОЛЕГ ПАНЧЕНКО

ІНФОРМАЦІЙНА БЕЗПЕКА В ЕПОХУ ТУРБУЛЕНТНОСТІ: ДЕРЖАВНО-УПРАВЛІНСЬКИЙ АСПЕКТ

Монографія

Київ
КВІЦ
2020

УДК 004.056.5(075.8)
DOI: 10.5281/zenodo.4011826
П16

Рекомендовано до друку: Вченою Радою Міжрегіональної Академії управління персоналом (протокол № 5 від 17.06.2020 р.); Науковою Медичною Радою Державного закладу «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України» (протокол № 2 від 14.05.2020 р.).

Рецензенти:

Бондаренко О.Г. – доктор наук з державного управління, доцент

Помаза-Пономаренко А.Л. – доктор наук з державного управління

Руденко О.М. – доктор наук з державного управління, доцент

П16 **Панченко О.**
Інформаційна безпека в епоху турбулентності: державно-управлінський аспект: монографія. К.: КВІЦ. 2020. 332 с.
ISBN 978-617-697-126-9

У монографії викладено погляд автора на інформаційну безпеку в причинно-наслідковому зв'язку з турбулентними явищами, що проявляються у всіх сферах життєдіяльності людини (природа, суспільство, інформаційне середовище). Проблема досліджується через призму державного управління, де центром цілепокладання є особистість. Введено ряд базових понять, розглянуто стан державного управління в умовах суспільно-інформаційної турбулентності, комунікаційні, правові, медико-психологічні аспекти забезпечення інформаційної безпеки.

Окрема увага зосереджена на інформаційній безпеці дитини. Розглянуто комплекс питань щодо протидії шкідливому впливу інформаційного середовища, удосконалення нормативно-правової бази з урахуванням закордонного досвіду.

Книга розрахована на широке коло науковців і практиків державного управління, менеджерів, викладачів і студентів, читачів, які цікавляться проблематикою державного управління з метою збереження суспільного порядку, підтримання психічного здоров'я населення в умовах турбулентних викликів.

УДК 004.056.5(075.8)
DOI: 10.5281/zenodo.4011826

ISBN 978-617-697-126-9

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 6

ВСТУП 8

РОЗДІЛ1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЕПОХУ ТУРБУЛЕНТНОСТІ

1.1. Епоха турбулентності: риси та ознаки 14
1.2. Потреби особистості в інформаційній безпеці 19
1.3. Суспільний запит на інформаційну безпеку 29
1.4. Суспільно значущі фактори державної інформаційної безпеки 35
1.5. Інформаційна безпека як складова національної безпеки держави 42
Список використаних джерел 53

РОЗДІЛ 2. СТАН ДЕРЖАВНОГО УПРАВЛІННЯ В УМОВАХ СУСПІЛЬНО-ІНФОРМАЦІЙНОЇ ТУРБУЛЕНТНОСТІ

2.1. Турбулентні явища та суспільні метаморфози як фактори ризиків державного управління 60
2.2. Соціальні інформаційно-психологічні аспекти в системі державного управління інформаційною безпекою в умовах турбулентності 70
2.3. Державні управлінські підходи до забезпечення інформаційної безпеки в умовах турбулентного стану сучасного суспільства 77
2.4. Стратегічні напрямки державної політики в умовах актуалізації інформаційних викликів епохи турбулентності 85
Список використаних джерел 98

РОЗДІЛ 3. КОМУНІКАЦІЙНА СТРАТЕГІЯ ЯК СКЛАДОВА ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ
3.1.Комунікаційні технології – джерело інформаційної безпеки 103
3.2. Значення мас-медіа в системі державного управління інформаційною безпекою 116
3.3. Засоби масової комунікації як платформа забезпечення державної інформаційної політики в сфері цифрової трансформації суспільства 129
Список використаних джерел 141

РОЗДІЛ 4. ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДИТИНИ В УКРАЇНІ
4.1. Інформаційні ризики безпеки дитини в турбулентному інформаційному середовищі 144
4.2. Міжнародні нормативно-правові документи щодо забезпечення інформаційної безпеки дитини 154
4.3. Державне управління інформаційною безпекою дитини 167
4.4. Ювенальна юстиція в забезпеченні прав дитини 174
Список використаних джерел 192

РОЗДІЛ 5. МЕДИКО-ПСИХОЛОГІЧНІ АСПЕКТИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ
5.1. Тривожні розлади людини в умовах турбулентності 202
5.2. Медико-психологічний супровід пацієнтів із тривожними розладами 214
5.3. Реабілітація як складова державної політики у сфері інформаційно-психологічної безпеки 242
Список використаних джерел 251

РОЗДІЛ 6. ЗАКОНОДАВЧІ ЗАСАДИ ТА ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
6.1. Система забезпечення інформаційної безпеки держави 256
6.2. Сучасні нормативно-правові документи у сфері забезпечення інформаційної безпеки 270
6.3. Правовий захист громадян у сфері інформаційної безпеки 276
Список використаних джерел 286

РОЗДІЛ 7. МЕТОДОЛОГІЧНІ АСПЕКТИ СТРАТЕГІЧНОГО УПРАВЛІННЯ ДІЯЛЬНІСТЮ СУБ'ЄКТІВ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
7.1. Сутність, мета та особливості стратегічного управління забезпеченням інформаційної безпеки 290
7.2. Інформаційна безпека органів державної влади як основа національної безпеки 300
7.3. Концептуальні засади визначення оптимальних шляхів щодо вдосконалення системи інформаційної безпеки України 314
Список використаних джерел 321

ВИСНОВКИ 325

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АТО – Антитерористична операція
АТ – Артеріальний тиск
ВООЗ – Всесвітня організація охорони здоров'я
ВРУ – Верховна Рада України
ДЗ «НПМ РДЦ МОЗ України» – «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України»
ЄЕС – Європейська економічна спільнота
ЄКПЛ – Європейська Конвенція із прав людини
ЄС – Європейський Союз
ЗМІ – Засоби масової інформації
ЗСУ – Збройні сили України
ІС – Інформаційне середовище
ІКТ – Інформаційно-комунікаційні технології
ІПБ – Інформаційно-психологічна безпека
ІБ – Інформаційна безпека
ІБД – Інформаційна безпека дитини
ІПБ – Інформаційно-психологічна безпека
ІТ –Інформаційні технології
КМУ – Кабінет Міністрів України
КРІ – Ключові показники ефективності
МІБ – Масово-інформаційна безпека
МКХ 10 – Міжнародний класифікатор хвороб
НАТО – Організація Північноатлантичного договору
НЛП – Нейролінгвістичне програмування
ОКР – Обсесивно-компульсивний розлад
ООН – Організація Об'єднаних Націй
ООС – Операція об'єднаних сил
ПТСР – Посттравматичний стресовий розлад
РНБО – Рада національної безпеки і оборони
СРСР – Союз Радянських Соціалістичних Республік
США – Сполучені Штати Америки

СНД – Співдружність Незалежних Держав
СК – Сімейні конференції
СЗІБ – Система забезпечення інформаційної безпеки
СІАЗ – Система інформаційно-аналітичного забезпечення
СБУ – Служба безпеки України
СЗРУ – Служба зовнішньої розвідки України
ТБ – Телебачення
ЦНС – Центральна нервова система
ЦОВВ – Центральні органи виконавчої влади
ЮНЕСКО – Організація Об'єднаних Націй з питань освіти, науки і культури

ВСТУП

Турбота про громадян була й залишається головною функцією держави на кожному історичному етапі її розвитку. При цьому будь-які зміни в парадигмі існування неодмінно ведуть до модернізації цілей і завдань держави та суспільства щодо убезпечення від внутрішніх і зовнішніх загроз. Незмінним залишається визнання людини як найвищої цінності держави.

Судячи з усієї сукупності глобальних екологічних, економічних, соціальних, політичних і культуральних процесів, можна стверджувати, що настала «епоха турбулентності», що характеризується нестабільністю як світової системи взагалі, так і суспільно-політичної ситуації в окремо взятій країні. Простежується синергетичний ефект накладення минулих (невирішених) проблем і нових глобальних викликів: один катаклізм «наповзає» на інший, міжкризові періоди скорочуються, а вихід із чергової кризи стає затяжним, більшість конфліктів не вирішується, а лише «заморожується». Існуючий баланс взаємин між людиною і природою, людиною і соціумом, соціумом і державою внаслідок турбулентних явищ порушується, у результаті – хаос і непередбачуваність подій.

Революційний за своїми темпами розвиток інформаційно-комунікаційних технологій призвів не тільки до зміни наукових підходів до пояснення новітніх подій, а й до суттєвої трансформації самого життя. Більшість дослідників схиляється до думки, що саме інформатизація суспільства призвела до прискорення появи нових тенденцій у світовому розвитку, адже інформація супроводжує всі сфери суспільних відносин. Хаотичні нелінійні процеси в суспільстві, у тому числі й інформаційного характеру, мають вирішальний вплив на життя сучасної людини. Особливого значення в турбулентному суспільстві набуває інформаційна безпека.

Отже, нові виклики сьогодення вимагають кардинальної трансформації напрямків розвитку державної системи

інформаційної безпеки, формування її концепції на нових методологічних засадах, які передбачають необхідність визначення цілей і завдань державної системи інформаційної безпеки, основних напрямків та механізмів її реалізації, результатів впливу державної інформаційної політики на соціально-економічний, політичний і культурний розвиток популяції.

Усе вищевикладене стало підґрунтям для дослідження інформаційної безпеки в епоху турбулентності, результати якого викладені в даній монографії.

Тема дослідження є актуальною для науки й практики публічного управління та адміністрування, а також медицини, психології, журналістики. Адже в умовах турбулентності актуалізуються й проблеми, що зазнали фрагментарного вирішення теоретичної основи державного управління у сфері інформаційної безпеки, зокрема: понятійно-категоріальний апарат дослідження; ідентифікація, класифікація та оцінювання ризиків інформаційній безпеці при прийнятті управлінських рішень; концептуальні засади формування системи забезпечення інформаційної безпеки; методологія стратегічного планування. Поряд із цим, уваги державного регулювання потребують система організації медико-психологічної допомоги, реабілітації, абілітації, координація супроводу пацієнтів із тривожними розладами внаслідок прогресуючої інформатизації, запровадження національних програм щодо підвищення інформаційної культури.

Основна ідея автора монографії – це систематизувати в читача вже наявні знання соціальних явищ, надати можливість чітко розставити акценти державного регулювання в інформаційно-прогресуючий час і забезпечити кожного розумінням особистісної інформаційної безпеки, що є невід'ємною частиною безпеки суспільної та національної.

Композиційна побудова монографічного дослідження визначена його метою та завданнями і складається з семи розділів.

У першому розділі *«Теоретико-методологічні засади інформаційної безпеки в епоху турбулентності»* розглядаються питання сутності, термінології та понятійного апарату, визначено проблему в різних ракурсах прояву та реакції на неї з боку державного управління. Проаналізовано риси та ознаки епохи турбулентності, відповідно визначено місце інформаційної безпеки в системі національної безпеки держави. Особлива увага приділена суспільному запиту на інформаційну безпеку, що на сьогодні є актуальною проблемою, адже сучасна людина, її повсякденне життя є залежними від інформаційного середовища. Почуття безпеки пов'язане зі станом миру, відсутністю страху. Безпека є національним завданням і полягає в підготовці як особистості, так і державних структур до інформаційних загроз. Для кожного суспільства питання безпеки є одним із основних вимірів його способу мислення про соціальну реальність.

У другому розділі *«Стан державного управління в умовах суспільно-інформаційної турбулентності»* висвітлені теоретичні основи державного управління в умовах суспільно-інформаційної турбулентності, систематизовані соціально-психологічні виклики в системі державного управління інформаційною безпекою. Наводяться різні приклади світової турбулентності, зокрема у вигляді коронавірусної інфекції COVID-19. Окремим питанням вивчено метаморфози в духовному житті, які виражені в зростаючому символічному насильстві, обумовленому комерціалізацією мас-медіа, і, як наслідок, викликають соціальну тривогу й невизначеність. Запропонована авторська модель підтримки рівноваги стану динамічної системи, що дозволяє окреслити ризики викликів епохи турбулентності та сформувати стратегічні напрямки державної інформаційної політики.

У третьому розділі *«Комунікаційна стратегія як складова державного управління інформаційною безпекою»* представлено значення інформаційно-комунікаційних технологій у сучасному суспільстві, а також визначено їх домінування в

інформаційній безпеці, у національній – взагалі. Викладено різні форми ведення соціального діалогу в ЗМІ. Доведено, що відкритий діалог використовують засоби масової інформації, що працюють над пошуком такого рішення (компромісу, консенсусу), який був би на користь усім, і не бояться «іншої сторони цієї медалі». На сторінках даного розділу також наведено класифікацію засобів масової комунікації, проаналізовано форми подачі інформації та визначено їхній вплив на державу, суспільство й особистість. Підкреслюється, що інформаційна сфера стала системоутворюючим фактором суспільного життя, тобто в життєдіяльності суспільства вона грає не допоміжну роль, а одну з ключових, у тому числі з точки зору державної політики та державного управління. Акцентується увага на таких напрямках державного регулювання інформаційної безпеки, як: забезпечення достовірності відомостей про соціально значимі події, недопущення підпорядкування ЗМІ, регулювання рівня концентрації та монополізації ЗМІ, удосконалення національного законодавства в частині гарантій свободи слова та інформації, вільного поширення масової інформації.

У четвертому розділі *«Засади формування системи державного управління у сфері інформаційної безпеки дитини в Україні»* визначені інформаційні ризики безпеки дитини в турбулентному інформаційному середовищі, наведено статистичні дані використання дітьми й підлітками інформаційних технологій, соціальних мереж і загального Інтернет-простору. Проаналізовано міжнародні нормативно-правові документи щодо інформаційної безпеки дитини. Наголошено, що дитина, будучи активним учасником суспільних відносин в інформаційній сфері, є найбільш незахищеним їхнім суб'єктом у силу вікового онтогенезу та підвищеної інформаційної вразливості, тому вона потребує особливого захисту з боку держави. Проблема інформаційної безпеки дітей є не менш актуальною і зумовлює вирішення комплексу питань, пов'язаних із упорядкуванням інформаційного простору України, поглибленням наукових

досліджень щодо протидії шкідливому впливу ЗМІ, удосконаленням нормативно-правової бази по відношенню до суб'єктів інформаційної діяльності. На вимогу цього запропонована державницька модель ювенальної юстиції.

П'ятий розділ *«Медико-психологічні аспекти державного регулювання інформаційної безпеки особистості»* присвячений проблемам розбудови й організації медико-психологічної підтримки особистості, і населення взагалі, на державному рівні. Важливість включення цього напрямку пояснюється тим, що порушення інформаційно-психологічної безпеки у вигляді шкоди психічному здоров'ю людини (інформаційно-психологічна турбулентність, тривога, страх, посттравматичний стресовий розлад) вимагають постфактумного реагування у вигляді, насамперед, медико-психологічної допомоги з акцентом на вирішення психологічних проблем і їх наслідків соматичного, психосоматичного і психічного ґенезу. Закладена не тільки теоретична основа для розробки дієвої державної політики щодо організації реабілітаційної допомоги особам, які мають збитки психічному здоров'ю, а й намічені практичні кроки реалізації.

У шостому розділі *«Законодавчі засади та правове забезпечення інформаційної безпеки»* приведено обґрунтування законодавчих засад та забезпечення правового захисту інформаційної безпеки. Розглянута система забезпечення інформаційної безпеки держави, зокрема визначено сучасний стан законотворчої діяльності у сфері інформаційної безпеки, представлені основні засади правового захисту громадян щодо інформаційної безпеки. Оскільки сучасний стан законодавчої основи інформаційної безпеки можна визначити як стан системи, що знаходиться в стадії формування, перед законодавцем стоїть складне завдання створити гнучку правову систему, яка могла б адекватно реагувати на економічні та соціально-політичні зміни в країні й за кордоном і водночас забезпечити необхідний рівень національної та інформаційної безпеки.

Останній, сьомий розділ *«Методологічні аспекти стратегічного управління діяльністю суб'єктів державного управління у сфері інформаційної безпеки»*, є логічним завершенням проведеної наукової роботи. Даний розділ присвячено концептуальним засадам визначення оптимальних шляхів удосконалення системи інформаційної безпеки України. Розглянуто наукові положення щодо визначення сутності, мети та особливостей стратегічного управління забезпечення інформаційної безпеки. Охарактеризовано інформаційну безпеку органів державної влади як основу сучасного державного управління. Наголошується, що стратегічне управління – це управління, що спирається на людський потенціал як основу організації, орієнтує виробничу діяльність на запити споживачів, гнучко реагує і проводить своєчасні зміни в організації, що відповідають виклику з боку оточення та дають змогу домагатися конкурентних переваг, що в сукупності дає можливість організації виживати в довгостроковій перспективі, досягаючи при цьому своїх цілей.

Інформаційна безпека – це організм, система, що буде робочою в тому випадку, якщо буде керованою. Очевидно, що інформаційна безпека завжди буде похідною від стратегії розвитку самої держави. Адже саме дії громадян, здійснення їхніх планів і способу життя повинна забезпечувати вдосконалена система інформаційної безпеки.

Представлене видання розраховано на широке коло науковців і практиків державного управління, менеджерів, викладачів і студентів, читачів, хто цікавиться проблематикою державного управління з метою збереження суспільного порядку, підтримання психічного здоров'я населення в умовах турбулентних викликів.

РОЗДІЛ 1

Теоретико-методологічні засади інформаційної безпеки в епоху турбулентності

1.1. Епоха турбулентності: риси та ознаки

За всіма економічними, політичними, екологічними, культурними, інформаційними ознаками людство вступило в епоху турбулентності, яка характеризується низкою важливих особливостей: плинність, нестійкість, невизначеність, і яка ставить перед суспільством до цих пір незвідані виклики. Серед науковців існує думка, що саме інформатизація суспільства призвела до прискорення появи нових тенденцій у світовому розвитку.

Поняття «турбулентність» у проекції на суспільні процеси з'явилося наприкінці XX століття після виявлення досить суворих закономірностей хаотичної поведінки не тільки фізичних, але й біологічних і «соціальних» об'єктів, економічних і політичних явищ. Представники соціальних і економічних наук почали вживати терміни «турбулентні часи», «турбулентний світ», «соціальна турбулентність», «турбулентний соціум» (наприклад, [1-5]). Отже, саме «епоха» (тривалий період, що виділяється за характерними явищами, подіями) більш доречна у зв'язці з турбулентністю [6].

Розов Н.С., визначаючи епоху турбулентності як певний історичний період в історії людства, стверджує, що в Європі таких періодів було шість [7]. Кожна з епох турбулентності еволюціонувала за допомогою затвердження нового міжнародного порядку, нових принципів внутрішньополітичного устрою держав, поширення нових релігійних, соціальних, моральних цінностей. Нинішню кризу глобальної стабільності вбачаємо в ряді ознак економічної, політичної, воєнної, екологічної та інших сфер діяльності людини.

У довгостроковій ретроспективі поточна критична ситуація представляється як черговий цикл геополітичного і геоекономічного переділу світу. Ключовим моментом тут є продовження розпаду біполярного світу і його перетворення на багатополярний, причому характер, геополітична структура, політична та економічна вага його окремих елементів змінюються невизначеним чином [8].

Для визначення поняття «епоха турбулентності» розглянемо декілька передумов. Термін «турбулентність» походить від латинського turbulentus – «бурхливий, хаотичний, невпорядкований». Його використання вказує на переважання нелінійних процесів, хаотичність, непередбачуваність подій, різкі зміни тенденцій, зростання конфліктності. При розгляді суспільних відносин таке визначення може бути використане для аналізу «порушень соціального порядку». Згідно з класичним визначенням, соціальний порядок – система, що включає індивідів, взаємозв'язки між ними, урегульовані соціальними нормами (право, мораль, релігія тощо), що сприяють поведінці людей, необхідній для успішного функціонування цієї системи.

Вочевидь, епоха турбулентності повинна зачіпати як мінімум два рівні соціальних порядків – усередині держави (економічний, політичний, культурний, інформаційний) і порядок міжнародний, тобто формальні й неформальні правила взаємодії між державами. Крім того, у відповідний концепт необхідно включити головні зовнішні прояви турбулентності: підвищення щільності конфліктів, у тому числі насильницьких, їх загострення й масштаб. Нарешті, епоха турбулентності має не тільки об'єктивний (кризи, конфлікти та інші деструктивні процеси), а й суб'єктивний аспект у вигляді масових проявів безвиході, утрати орієнтирів, відсутності видимих шляхів подолання негараздів [9].

Враховуючи сказане, а також беручи до уваги попередні дослідження, формулюємо наступне визначення: епоха турбулентності – це історичний період, коли частішають і загострю-

ються економічні та соціально-політичні конфлікти із характерним зростанням насильства у вигляді війн, революцій, тероризму; відчуття краху колишнього стабільного стану, бурхливих суперечливих емоцій (від утопічних надій до розгубленості й песимізму), що ведуть до істотного порушення психічного здоров'я населення, внутрішнього соціального порядку в державі, а також порядку та форм міжнародних відносин.

У масштабах держави причини турбулентності можуть бути як внутрішніми процесами, зумовленими, у тому числі, факторами світової турбулентності, так і зовнішніми – цілеспрямованими інформаційними впливами недружніх країн із метою дестабілізувати суспільно-політичну ситуацію, викликати нестабільність і хаос.

Внутрішнім джерелом енергетичного збурення як причини турбулентності є, у першу чергу, протистояння еліт у боротьбі за владу й політична «незадоволеність» населення. Особливо яскраво цей процес спостерігається під час виборів і зміни правлячих еліт. І саме держави з демократичною формою правління, яким властиві свобода слова й плюралізм, найбільш уразливі в плані виникнення турбулентності [10].

Кожну людину можна розглядати як «соціальну частку», аналогічну окремим молекулам рідини в проточній системі. Коли енергія в системі низька, тобто коли є загальне задоволення або, принаймні, мовчазна згода з керівництвом держави, суспільство «тече» в стаціонарному й корисному режимі (за аналогією з ламінарним потоком). Коли ж енергія в системі висока (присутнє велике політичне розчарування), виникає турбулентність, яка може пошкодити «канал спілкування», (тобто соціальні інститути та інші механізми соціального упорядкування). За наявності мільйонів соціальних часточок завжди буде великий сегмент населення, яке потерпає від політичного розчарування. Соціальні частки, що «не відбулися», за достатньої енергетики перетнуть поріг турбулентності системи, створюючи соціальні

вири й вихори, які порушують плавну течію суспільства. Боротьба ж еліт може перетворитися в «політичне торнадо».

У демократичному суспільстві, де влада знаходиться в руках багатьох політичних діячів (тобто «народу»), практично неможливо передбачити, куди воно буде йти протягом тривалого часу. До того ж, маси часто дуже легко можуть «похитнути» демагогами і популістами, що загрожує рухом суспільства в абсолютно непередбаченому напрямку.

Демократичні інститути демонструють більшу чутливість до початкових умов («ефект метелика»). У той час, як демократична держава може теоретично бути передбачуваною на основі її поточного стану, навіть невеликі зміни можуть призвести до несподіваної політичної поведінки.

Енергія, що «запечена» в систему, у кінцевому результаті призводить до її нестійкості й повинна знайти реалізацію, як правило, у міжетнічному або міжпартійному насильстві, або в революції, що призводить до більш авторитарної, із більш низькою енергією системи [11].

Серед найбільш суттєвих факторів виникнення критичної точки турбулентності можна назвати економічний, природний, культурний, політичний, інформаційний. Щодо останнього, слід зазначити, що інформаційне середовище (ІС) – це не тільки сфера людської життєдіяльності, що найбільш динамічно розвивається, але й та, що практично одноосібно диктує умови розвитку сучасного суспільства. Динамізм змін, складність і неоднозначність ІС, а також невизначеність, непередбачуваність і нестабільність породжують синергетичний ефект, що обумовлює об'єктивний характер виникнення деструктивних чинників, які ускладнюють процес адаптації до змін, що відбуваються. Тому дослідження явищ інформаційної турбулентності та її наслідків у соціально-психологічній площині є важливим із точки зору вироблення державної стратегії забезпечення інформаційно-психологічної безпеки.

Стан ІС, із яким сучасне суспільство нероздільно пов'язане, значно впливає на світовий суспільний розвиток. У джерелі [12] розглядаються три можливі сценарії:

– *перший сценарій* полягає в тому, що для того, щоб витримати турбулентність, люди або роблять якісь дії, які знімають напругу, або адаптуються до напруженого середовища. Якщо турбулентність не закінчується або посилюється, вони поступово втрачають здатність до позитивної адаптації. Люди вибирають таку реакцію на напругу, яка призводить до їхньої деградації. Вони починають придушувати реальність, заперечуючи саме її існування, і все більше перебувати в інфантильних фантазіях, що дозволяють їм упоратися зі стресом. Відбувається переоцінка цінностей на користь менш гуманних і більш тваринних. До речі, про це попереджається і в [13]: «можливий і соціальний ароморфоз, розщеплення людства на підвиди: людей нової свідомості, носіїв високої культури, і людей, які повертаються до зоопсихологічних форм буття».

– *другий сценарій* – сегментація суспільства, коли кожна група (етнічна, расова, гендерна) воює проти всіх інших. Нації розпадаються на регіональні групи, які, у свою чергу, дробляться на ще більш дрібні етнічні групи заради спрощення процесу прийняття рішень. Природні лінії поділу суспільства перетворюються на барикади.

– *третій сценарій* передбачає відхід індивідів до свого особистого світу і відмову від усіх соціальних зв'язків, які могли б долучити їх до чужих справ.

Підбиваючи підсумки за цими сценаріями, слід констатувати, що якоюсь мірою їхні ознаки конкретно підтверджуються сьогоднішніми реаліями. Щоб зрозуміти, що відбувається з суспільством в умовах турбулентності, потрібні серйозні фундаментальні дослідження, яких зараз украй мало.

Із огляду на викладене, випливає, що першочерговим стратегічним завданням держави є забезпечення національної єдності, включаючи соціальні, економічні, культурні, інформа-

ційні аспекти. Поряд із цим, для подолання турбулентності й досягнення керованості необхідна систематизація та алгоритмічне використання відповідних суспільно-державних механізмів.

1.2. Потреби особистості в інформаційній безпеці

Історичний досвід свідчить, про те, що з моменту зародження життя на нашій планеті, людина в процесі свого існування й розвитку завжди прагнула до різних потреб (бажань), у тому числі й у сфері безпеки. Поняття «потреба» в сучасних умовах стало тим, безперечно, престижним, позитивним, необхідним, що створює умови для вдосконалення та розвитку людини. Власне, потреби формуються у процесі життєдіяльності за певного відчуття незадоволеності, і вони є вельми різноманітними. Як казав Демокріт: «Людина не знає кордонів своїх потреб». Вони можуть із часом змінюватися: одні йдуть, інші з'являються. Що взагалі-то природно. Але найголовніше – вони мають бути задоволені. У цьому полягає сутність потреб.

Аксіоматично слід визнати, що людське життя складається з потреб та їх задоволення. У цьому випадку ми можемо говорити про відчуття щастя. В іншому випадку – відбувається порушення психологічного комфорту, зниження соціального функціонування людини, розвиток психічних розладів та антидержавних проявів.

Вивчення потреб людини пов'язано з важливими проблемами сучасного суспільства. Людина – істота біосоціальна, і в її становленні та розвитку як соціальної істоти визначальними є соціальні фактори. Система соціальних потреб мобільно впливає на поведінкові реакції різних соціальних груп, посилюючи або послаблюючи їх активність. Еволюція у сфері потреб стала дієвим чинником змін в економічних відносинах, політиці, ідеології, чинником перегляду життєвих цінностей і прагнень. Ці обставини вимагають уважного вивчення динаміки потреб із метою прогнозування соціальних змін та управління ними.

Володіння інформацією є однією з основних потреб особистості, без неї неможливе формування та існування індивідуальної свідомості, так як сучасна людина живе в епоху турбулентного розвитку інформаційних технологій та постійного інформаційно-психологічного впливу на особистість, суспільство і державу.

Акцентуація на інформаційно-психологічному аспекті безпеки особистості, суспільства і держави сьогодні не випадкова, у зв'язку з подіями, що відбуваються у світі (кризи, військові конфлікти, кібератаки, загрози гібридних війн), набуває особливого значення та безпосередньо стосується духовної сфери життєдіяльності людини. Важливим є дослідити потреби особистості в інформаційній безпеці в умовах турбулентної сучасності. Збереження інформаційної безпеки людини, її психологічного здоров'я, пошук ефективних методів розв'язання даної проблеми є важливим і актуальним питанням державної інформаційної політики [14].

Обґрунтованим у науці є той факт, що людина, її спрямованість передусім визначаються її потребами, бо останні формують діяльність людини, її вчинки, пояснюють мотиви, інтереси й цінності. Сутність «потреби» в літературі трактується по-різному [15, 16]. З одного боку, потреба – це необхідність людини в чому-небудь, що відчувається у вигляді психологічного та фізичного дискомфорту. З іншого боку, потреба – це стан людини, що складається на основі суперечності між наявним і необхідним (або тим, що здається людині за необхідне) і спонукає її до діяльності задля усунення даної розбіжності.

Потреби – це динамічна система, що знаходиться в розвитку та під час якої відбувається їх трансформація, перехід одних потреб в інші, їх зміна. Потреби людини виступають важливими мотивами для її повсякденної діяльності. Це пояснюється тим, що будь-яка потреба – це завжди суперечність між тим, що людина має, і тим, до чого вона прагне. Вони спонукають людину до прояву активності та пошуку шляхів їх задоволення,

стають внутрішніми збудниками діяльності. Розрізняють потреби суспільства та особистості. Потреби людини так само різноманітні, як багатогранна її суспільна та індивідуальна діяльності, що, власне, є зображенням тих усіляких суспільних відносин, у яких вона перебуває [17, 18]. Разом із тим, усі потреби людини, вочевидь, перебувають у певній кореляції – координації та субординації. Одні потреби виступають базовими для людини, інші – надбазовими. Тобто існують першочергові, основні потреби й ті вищі, що формуються на їхньому підґрунті за умови повного або умовно-достатнього задоволення. Індивідуальні потреби є не тільки елементом системи суспільних потреб, але є також системою, що складається з певних взаємопов'язаних елементів.

Також людські потреби формуються життєвим простором, бажанням до змін. З одного боку, це призводить до виходу із зони комфорту, тим самим спонукаючи до чогось нового, отримання бажаного, з іншого – існує потреба у стабільності та побоювання перед рухом до змін. Звідси і виникає основна потреба людини в безпеці.

Слід відмітити, що існують різні типології людських потреб [19]. За наявності багатьох класифікацій потреб, усі вони зводяться до виділення природних (біологічних) і соціальних (культурних) потреб. Однак найвідомішою з них є «піраміда потреб» американського психолога А. Маслоу, де він згрупував безліч людських потреб. У своїй роботі «Мотивація та особистість» (1954) Маслоу [20] припустив, що всі потреби людини вроджені і що вони організовані в ієрархічну систему пріоритету або домінування, що складається з п'яти рівнів (рис. 1.1.).

Зазначена піраміда А. Маслоу включає наступні рівні потреб:

1. Фізіологічні потреби (їжа, вода, сон тощо);
2. Потреба в безпеці (стабільність, порядок, залежність, захист, свобода від страху, тривоги і хаосу);

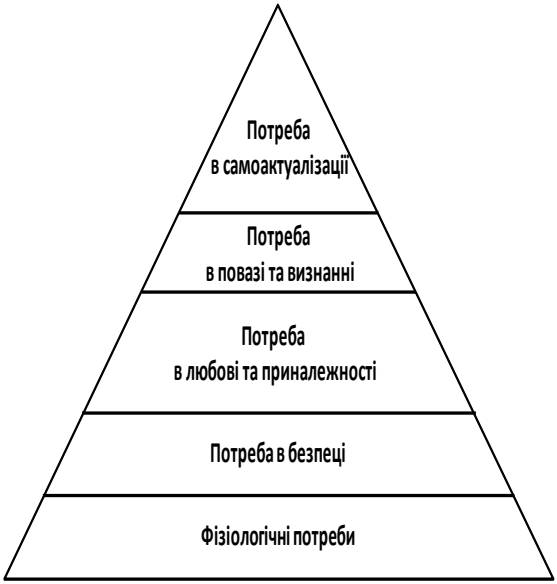


Рис. 1.1. Ієрархія потреб за А. Маслоу

3. Потреба в любові та приналежності (сім'я, дружба, своє коло, референтна група);

4. Потреба в повазі та визнанні (я поважаю себе, шанують мене, я відомий і потрібний, я досягаю, престиж і репутація, статус, слава);

5. Потреба в самоактуалізації (розвиток здібностей, людина повинна займатися тим, до чого в неї є схильності та здібності);

Але за дві третини століття відбулася суттєва трансформація інформаційного суспільства, демінімізувалася структура бажань і потягів, що включають у себе більш широкий діапазон потреб сучасної людини, а тому виникла нагальна потреба вдосконалення концепції відносно запиту сьогодення.

Модернізована піраміда людських потреб уміщує 7 рівнів (рис. 1.2.) [21].

Рис. 1. 2. Модернізована О. Панченком піраміда людських потреб А. Маслоу

Зміст кожного з рівнів:

1. Фізіологічні потреби (спрага, голод, тепло, комфорт, сон, секс, релакс) є вродженими та властиві всім людям. Їх задоволення необхідне для підтримки життя, виживання, тому їх нерідко називають біологічними потребами.

2. Під потребою у безпеці мається на увазі (рис. 1.3.) фізична (охорона здоров'я, безпека на робочому місці, у громадських місцях, удома), правова (захищеність, стабільність, потреба в Законі та його виконанні, упевненість), психологічна (психоемоційний комфорт), економічна (грошовий дохід, гарантованість робочого місця, державний соціально-економічний

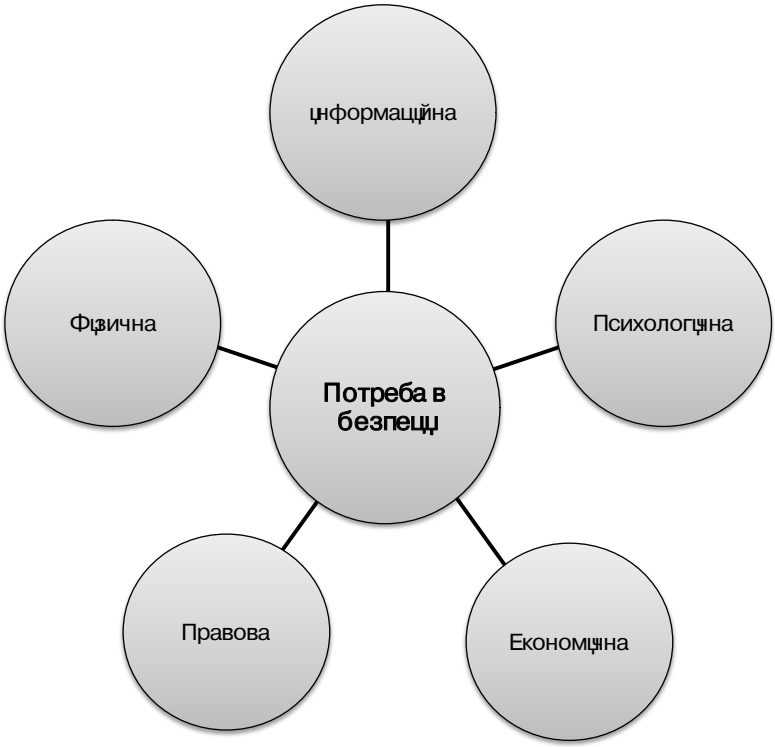


Рис. 1.3. Види потреб у безпеці

захист – заробітна плата) та інформаційна (отримання й надання достовірної інформації, захист від фейків і вбросів, інформаційних атак) [22]. Задоволення потреб у безпеці забезпечує впевненість у завтрашньому дні. Потреба в різних видах і формах безпеки існує на всіх етапах розвитку людства, однак саме в умовах турбулентності вона набуває статусу національної (і навіть транснаціональної) ідеї [23]. Для підтримки громадського порядку важливою виступає наявність потреби в Законі, його дотриманні. Тільки маючи мотив, у людини виникає потре-

ба, а якщо існує потреба, то буде відбуватися пошук шляхів її задоволення.

3. Потреба в прихильності (бути визнаним і прийнятим людьми, бути чиїмось, мати турботу та підтримку). Ця потреба орієнтується на спілкування і емоційні зв'язки з іншими: дружбу, любов, приналежність до групи та прийняття нею. Люди – істоти соціальні, колективні, а тому відчувають бажання подобатися іншим і спілкуватися з ними.

4. Потреба в повазі (потрібність, значимість, схвалення, визнання). Відносяться потреби як у самоповазі, так і в повазі з боку інших, у тому числі потреби в престижі, авторитеті, владі. Самоповага зазвичай формується при досягненні поставленої мети, вона пов'язана з наявністю самостійності та незалежності. Потреба в повазі з боку інших людей орієнтує людину на завоювання та отримання суспільного визнання, репутації.

5. Пізнавальні потреби (знати, уміти, розуміти, аналізувати, творити). Розглядаються такі потреби як у пізнанні нового, у самопізнанні, потреби в орієнтації, вони пов'язані з інтелектуальним пізнанням світу, зі спілкуванням, з осмисленням власного життя. Засобом задоволення пізнавальної потреби завжди є нове знання, нова інформація. При цьому отримання нового знання не гасить її, а, навпаки, підсилює. Пізнавальна потреба в розвинутій формі стає ненасиченою – чим більше людина дізнається, тим більше їй хочеться знати.

6. Естетичні потреби (гармонія, краса, радість, любов, симетрія, порядок) виражаються в зацікавленості людини в естетичних цінностях. Зовні потреби в естетичному задоволенні можуть проявлятися дуже схоже – у прагненні до порядку, симетрії, закінченості, структурованості, системності.

7. Мотивація для найбільшої реалізації особистісних можливостей – самоактуалізація (мораль, духовний ріст, особистісний розвиток, визнання фактів, реалізація своїх цілей). Під цією потребою мається на увазі бажання та прагнення людини до найповнішого виявлення, розвитку та втілення своїх особистіс-

них можливостей, зростання. Потреби в самоактуалізації – це потреби зростання, яке може бути безмежним.

Відповідно до піраміди, сім основних рівнів потреб утворюють ієрархічну структуру, що як домінанта визначає поведінку людини. Потреби вищих рівнів не мотивують людину, поки не задоволені, принаймні частково, потреби нижнього рівня. Зазвичай ці групи потреб визначають соціальну поведінку людей своїм інтегральним впливом, вносячи більший або менший внесок у мотиви людини в залежності від умов його життя та індивідуальних особливостей особистості. У певні періоди часу та за відповідних умов одна з базових груп потреб може ставати провідною більшою мірою, ніж інші, визначаючи поведінку та діяльність людини. У зв'язку з цим вона може перебудовувати всю мотиваційну сферу особистості.

Як правило, за відносно стабільних соціальних умов потреба в безпеці досить добре влаштованої людини, принаймні в мінімальному ступені, задоволена або суб'єктивно сприймається як задоволена. У таких випадках у якості активного чинника детермінації мотиваційної сфери людини вона практично не фіксується і може проявлятися, наприклад, як перевага знайомих форм поведінки та життєвих ситуацій із цілком певними (досить чіткими) перспективами перед тими, у яких багато елементів невизначеності, прагнення до більш стабільних умов існування та ін.

Потреба в безпеці стає домінантною в умовах турбулентних явищ, які руйнують звичні стереотипи поведінки та сформований образ життя. Саме вона починає визначати мотивацію соціальної поведінки людини, перебудовуючи та змінюючи її, специфічним чином трансформуючи інші базові групи потреб, психічні особливості та характеристики особистості. Вона стає активним і переважним мобілізатором ресурсів організму людини в надзвичайних обставинах – соціальної дезорганізації, катастрофічних явищ природи, злочинних посягань та ін. Відсутність адекватних можливостей для задоволення цієї потре-

би викликає в особистості емоційно негативні, гостро пережиті психічні стани, на тлі яких протікають практично всі психічні процеси людини [24, 25].

Вплив інформації на особистість безперечний та очевидний. Людина в своєму існуванні не може обходитися без інформації, причому дана потреба зумовлена, у першу чергу, біологічною потребою в безпеці, орієнтацією в навколишньому середовищі, а потім уже у виборі моделей поведінки і реакції на інформаційний контент [26]. Інформація надходить до людини через сенсорні системи, що здатні диференційовано сприймати різноманітні стимули зовнішнього світу і внутрішнього стану самого організму людини і його психіки.

У будь-якому суспільстві інформація виконує такі основні функції: інтегративну – згуртування членів суспільства й соціальних груп; комунікативну – спілкування та взаєморозуміння; інструментальну – участь в організації виробництва та управління; пізнавальну – установлення об'єктивних закономірностей природи, суспільства, мислення. Суспільство є цілісною багатофакторною системою, що скріплюється наявністю засобів накопичення, використання, зберігання та передачі інформації. У суспільстві, занадто великому для прямих безпосередніх контактів, такими засобами руху інформації стають преса, книжки, радіо, телефонний зв'язок, телеграф, пошта та інші засоби комунікації [27].

Потреба в інформації обумовлена тим, що людині як істоті соціальній необхідна взаємодія з іншими людьми, інакше (в даному випадку від нестачі відомостей) настає дезорієнтація, соціальна дезадаптація, а також емоційна депривація, інформаційний голод і навіть інформаційний невроз. Однак надлишок інформації, швидкість її надходження в сенсорні системи, її сенс і значення для самої особистості є одним із факторів виникнення в людини стресових розладів, а в ситуації надзвичайних подій посттравматичного стресового розладу.

Отже людина змушена виробляти механізми захисту від впливу зовнішнього інформаційного середовища з метою забезпечення інформаційно-психологічної безпеки, оскільки поряд із інформацією, що адекватно відображає факти, там циркулює і деформована, перекручена інформація, часто створена спеціально для введення в оману при досягненні певних цілей. Що стосується безпеки особистості, то цілком очевидно те, що як і в біологічній, так і в соціальній природі людині всюди чатує небезпека, оскільки вона є складно організованою відкритою системою, до найважливіших психічних станів якої відносять небезпеку і безпеку [28]. Інформаційно-психологічна безпека особистості розглядається як стан захищеності психіки від дій, які впливають на неї, різноманітних інформаційних факторів, що перешкоджають чи ускладнюють формування і функціонування адекватної інформаційно-орієнтовної основи соціальної поведінки людини і в цілому життєдіяльності в сучасному суспільстві [29].

Недостатньо якісне інформаційне забезпечення, обмеженість в інформації або низька якість інформації призводить до руйнівних змін психіки людей, які проявляються в підвищенні психічної напруженості та неадекватній соціальній поведінці, що є наслідком відсутності достатніх можливостей для соціального орієнтування людини в навколишній ситуації та розуміння напрямків її розвитку, тобто в неможливості отримання соціально значущих даних у великому інформаційному потоці. Подібні речі значною мірою прослідковуються в ситуаціях умисного використання інформації для маніпулювання людьми, їхньою поведінкою. Почасти інформаційна безпека полягає в отриманні в достатньому обсязі даних для орієнтації в соціумі, що виступає однією з необхідних умов для соціально-психологічної адаптації особистості, її пристосування до актуальних суспільних змін.

Розглядаючи безпеку крізь призму державного управління, варто відзначити, що вона полягає не тільки у відсутності загроз, які суб'єктивно сприймаються окремими особами та

групами, а й у готовності особистості та державних структур до цих загроз. До державних інформаційних загроз відносять комп'ютерну злочинність та комп'ютерний тероризм, розголошення конфіденційної інформації, яка є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави, спроби маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації, поширення засобами масової інформації культу насильства, жорстокості, порнографії. Серед ризиків інформаційної безпеки особистості в цьому контексті може бути втручання в особисте життя, використання об'єктів інтелектуальної власності, обмеження доступу до інформації, протиправне використання засобів, що діють на підсвідомість, а також дезінформація, спотворення інформації.

Функціонально інформаційна безпека, як і інші аспекти безпеки людини, спрямована на реалізацію прав і свобод, потреб, інтересів, прагнень особистості, підвищення якості життя, включаючи суб'єктивне відчуття захищеності, забезпечення можливостей особистісного розвитку й самореалізації. На рівні особистості інформаційна безпека повинна забезпечити захищеність психіки і свідомості людей від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукання до самогубства.

Отже, ураховуючи темп сучасного життя й техногенного розвитку, життєві потреби сучасної людини суттєво змінилися і розширилися, зріс попит на безпечну життєдіяльність та інформаційно-психологічний комфорт задля особистісної реалізації в умовах турбулентного розвитку, інформаційної навали та несистемного суспільного хаосу.

1.3. Суспільний запит на інформаційну безпеку

Найважливіша роль у розвитку сучасного суспільства належить інформатизації, особливість якої полягає в тому, що од-

ним з основних видів діяльності членів суспільства є процеси, пов'язані з інформацією. Інформаційне суспільство, до якого неухильно прагне людство, докорінно змінює статус інформації, розширюючи її потенціал як позитивного ресурсу, так і виявляючи її різко негативні можливості. Інформація завжди оточувала людину, тому будь-яке суспільство можна вважати інформаційним.

Однак впровадження сучасних інформаційних технологій у сфери життєдіяльності (культурну, соціальну, економічну, політичну) істотно підвищило залежність суспільства й кожного конкретного індивіда від надійності функціонування інформаційної інфраструктури, достовірності використовуваної інформації, її захищеності від несанкціонованої модифікації, а також протиправного доступу до неї.

Сучасна людина, її повсякденне життя виявилися залежними від масової комунікації. Поширення мережевих комп'ютерних технологій, мобільного зв'язку та мережі Інтернет, інформаційні ресурси сучасного суспільства можуть нести не тільки благо, але й піддаватися зростаючій кількості загроз, що може надати шкоду інтересам особи, суспільства, держави, призвести до економічних збитків, тим самим ставлячи під загрозу безпеку національної інформаційної безпеки. У зв'язку з цим надзвичайної вагомості набуває питання запиту суспільства на інформаційну безпеку.

Вітчизняним і зарубіжним науковим дослідженням властива багатосторонність висвітлення питань інформаційної безпеки, у той же час відсутність єдиної концепції інформаційної безпеки держави як складової розвитку суспільних відносин, що свідчить про недостатній рівень розробленості теми. Велика кількість науковців і практиків [30-33], згідно до вимог сучасного стану соціуму, розробляють проблеми безпеки розвитку і функціонування держави, суспільства й особистості. Вони обґрунтовують положення про те, що стан інформаційної безпеки такої соціальної системи, як суспільство, безпосереднім чином

залежить від забезпечення потреб та інтересів соціальних груп і людини. Збільшення шансів у соціальній системі, яка прагне підвищити рівень своєї безпеки, досягається при першочерговому захисті інтересів людини. Важливо вказати, що дослідники відходять від принципу пріоритетності окремих складових національної безпеки в залежності від ситуації, згідно з їхньою точкою зору, шлях до безпеки знаходиться тільки в єдності основних сфер життя суспільства. Зазначені дослідження стали підґрунтям для наших досліджень.

Із позиції суспільних відносин безпекою можна назвати стан, у якому людина має відчуття впевненості та захищеності, почуття довіри до іншої особи або правової системи.

Основу інформаційної безпеки становить поведінка соціального суб'єкта, який ясно усвідомлює свої права й обов'язки. При цьому система морально-етичних норм виступає в якості керівництва безпечного застосування інформаційних технологій і формування суспільних відносин в інформаційній сфері. У забезпеченні безпеки інформаційних технологій на перший план виходить інформаційна етика, що спрямована на інформування кожного соціального суб'єкта про його права та обов'язки в інформаційному суспільстві, відповідальність за створення і використання інформаційно-комп'ютерних технологій та інших форм інформації.

Українська держава включена в процес загальної інформатизації суспільства і формування єдиного світового інформаційного ринку. Такі перетворення призвели до того, що в даний час усе більш актуального характеру набуває забезпечення інформаційної безпеки як невід'ємного елементу її національної безпеки, а захист інформації перетворюється на одне з пріоритетних державних завдань. Проблема створення й підтримки захищеного середовища інформаційного обміну, що обумовлює певні правила й політику безпеки сучасної держави, є досить актуальною, оскільки сьогодні головним стратегічним національним ресурсом, основою економічної та оборонної

могутності держави стає інформація та інформаційні технології. Інформація в сучасному світі є таким атрибутом, від якого у визначальному плані залежить ефективність життєдіяльності сучасного суспільства. Інформаційні технології принципово змінили обсяг і важливість інформації, її потік у технічних засобах зберігання, обробки й передачі. Загальна комп'ютеризація основних сфер діяльності призвела до появи широкого спектру внутрішніх і зовнішніх загроз, нетрадиційних каналів утрати інформації і несанкціонованого доступу до неї.

Із точки зору державного управління, інформаційна безпека розглядається як:

1) стан захищеності життєво важливих інтересів особи, суспільства й держави, при якому зводиться до мінімуму нанесення шкоди через неповність, несвоєчасність та неправдивість інформації; деструктивний її вплив; неправомірне використання та поширення персональних даних;

2) стан захищеності національного інформаційного простору, що забезпечує формування, використання й розвиток останнього в інтересах громадян, організацій, держави [34, 35].

Доцільно виділити наступні види інформаційної безпеки (рис.1.4.)

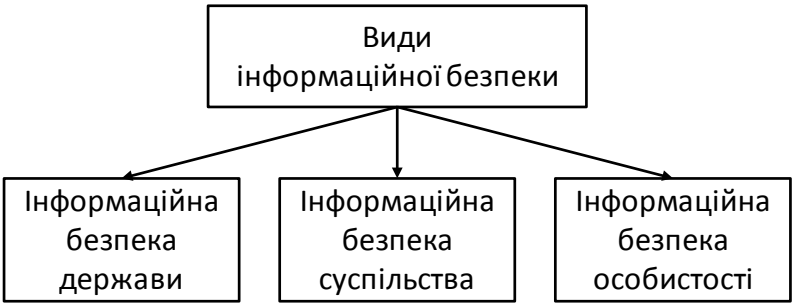


Рис. 1.4. Види інформаційної безпеки

Розглянемо більш детально кожний вид інформаційної безпеки:

Інформаційна безпека держави стан збереження інформаційних ресурсів держави й захищеності законних прав особистості й суспільства в інформаційній сфері. Іншими словами, інформаційна безпека держави це такий стан держави, при якому не може бути завдано шкоди його інформаційному середовищу за допомогою використання інформаційних ресурсів і систем. Інформаційна безпека держави це складова частина національної безпеки країни, забезпечення якої здійснюється шляхом комплексної організації всіх ресурсів і систем.

Інформаційна безпека суспільства це стан суспільства, у якому йому не може бути завдано істотної шкоди шляхом впливу на його інформаційну сферу. Інформаційна безпека суспільства може досягатися як в результаті проведення заходів, спрямованих на підтримку найбільш інформаційного середовища в безпечному стані для захисту об'єкта, захист об'єкта від деструктивного впливу, так і шляхом зміцнення імунітету й розвитку здатності суспільства і його членів ухилятися від руйнівного інформаційного впливу.

Безпека є однією з основних людських потреб, тобто є дуже важливою для суспільства. Почуття безпеки повинно бути пов'язане зі станом миру, відсутністю страху. Для кожного суспільства питання безпеки є одним із основних вимірів його способу мислення про соціальну реальність [36].

Інформаційна безпека особистості – стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Інформаційна безпека особистості в сучасному суспільстві постає як нагальна проблема, яка потребує комплексного та системного вирішення. Вирішення проблеми забезпечення інформаційної безпеки суспільства та особистості повинно но-

сити комплексний системний характер і здійснюватися на різних рівнях (рис. 1.5.):

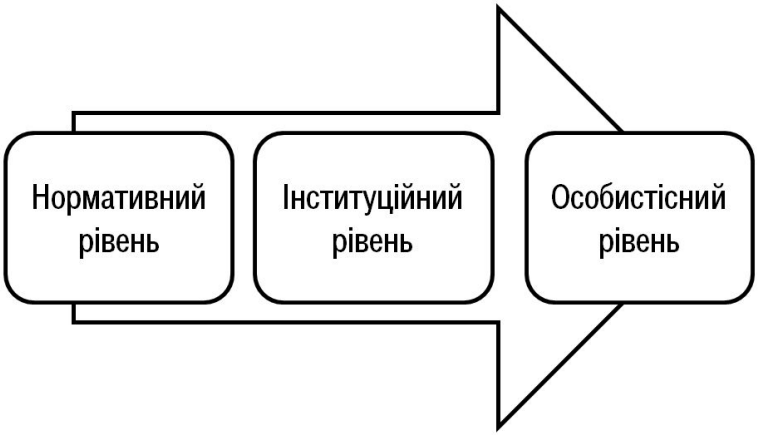


Рис. 1.5. Рівні забезпечення інформаційної безпеки суспільства та особистості

– перший рівень – нормативний.

Повинна бути створена несуперечлива нормативна база, що враховує всі аспекти проблеми інформаційної безпеки;

– другий рівень – інституційний, що має на увазі узгоджену діяльність різних соціальних інститутів, пов'язаних із вихованням і соціалізацією;

– третій рівень – особистісний, що пов'язаний, перш за все, із самовихованням, самоосвітою, формуванням високого рівня інформаційної культури особистості як частини загальної культури людини. На даному рівні відбувається формування необхідних особистісних якостей щодо забезпечення інформаційного самозахисту особистості.

Інформаційна безпека, виходячи з двоєдиної сутності інформації, повинна бути спрямована як на захист об'єктивної, так і суб'єктивної її складової.

У першому випадку вона виступає у вигляді безпеки інформації, у другому – у вигляді інформаційно-психологічної безпеки.

Ураховуючи той факт, що суспільні відносини в умовах інформатизації суспільства складаються і змінюються надзвичайно швидко, суспільство повинно навчитися адекватно реагувати на ці зміни, приводячи суспільні відносини відповідно до потреби реалій, попереджаючи появу небажаних для суспільства процесів. Для держави важливо мати сучасну концепцію входження в інформаційне суспільство. Вона повинна принципово відрізнятися від концепцій попередніх періодів розвитку держави, що були б орієнтовані в першу чергу на технічне забезпечення суспільних процесів.

На рівні суспільства й держави інформаційна безпека покликана забезпечити захищеність і, як наслідок, стійкість основних сфер життєдіяльності (економіки, науки, сфери державного і військового управління, а також суспільної свідомості) від небезпечних, дестабілізуючих і деструктивних інформаційних впливів.

1.4. Суспільно значущі фактори державної інформаційної безпеки

Внутрішніми і зовнішніми аспектами національної безпеки є інформаційна безпека, що покликана надійно захищати культурне надбання країни, інтелектуальну власність господарюючих суб'єктів і громадян, а також спеціальні відомості, що становлять державну і професійну таємницю. Тому розвиток будь-якої держави як суверенної, демократичної, правової та економічно стабільної можливий лише за умови забезпечення інформаційної безпеки всіх суб'єктів інформаційних відносин.

Практичного значення набуває аналіз суспільно значущих факторів державної інформаційної безпеки як позитивного, так і негативного характеру, що є реальними умовами здійснення

правового регулювання, становлення громадянського й інформаційного суспільства, розбудови правової держави, забезпечення національної та інформаційної безпеки з метою вироблення ефективних моделей державного управління та адекватних форм і методів здійснення державної влади.

Визначаючи фактори державної інформаційної безпеки, слід ураховувати взаємозв'язок базових понять «інформація», «інформаційна безпека» та «інформаційна культура». Інформація має властивість амбівалентності, тобто виступає одночасно у вигляді двох реальностей: об'єктивної та суб'єктивної. Згідно з першою, інформація носить або атрибутивний, або функціональний характери. Згідно з іншою, інформація – компонент нашого буття, реальність, але не об'єктивна, а суб'єктивна, така, що відноситься до області ідеального. Вона не матеріальна – це спалах свідомості, що породжує образ реального світу.

В іншій термінології, що вживається деякими дослідниками, інформація має дві сторони: змістовну і показну [36]. Суть змістовної сторони інформації – віддзеркалення у свідомості людини навколишньої дійсності, включаючи повідомлення, у формі психічних відчуттів. Ця сторона інформації залежить від фізіологічних особливостей рецепторів людини, її нервової системи, наявного досвіду осмислення тих або інших відчуттів, а також досвіду фіксації пізнавальних образів у мові, що веде до виникнення понятійного мислення. Суть показної сторони інформації визначають самі повідомлення, що передають психічні емоційні відчуття іншим людям. Показна сторона інформації залежить від здатності людини описувати свої відчуття окремою мовою, перетворювати описи в повідомлення й передавати їх іншим людям. Перетворення показної сторони інформації в змістовну і навпаки складає суть загального закону поширення інформації.

Важливою складовою показної сторони інформації є інформаційне середовище, що має дві складові: організаційну і технологічну. Організаційна складова включає виробництво

засобів інформатизації й інформаційних послуг, інформаційний ринок, підготовку й перепідготовку кадрів, проведення наукових досліджень. Технологічна складова інформаційної інфраструктури утворюється інформаційно-телекомунікаційними системами.

Основними принципами інформаційної безпеки є забезпечення конфіденційності, доступності, цілісності й автентичності інформаційних ресурсів та інфраструктури, що її підтримує (рис. 1.6.).

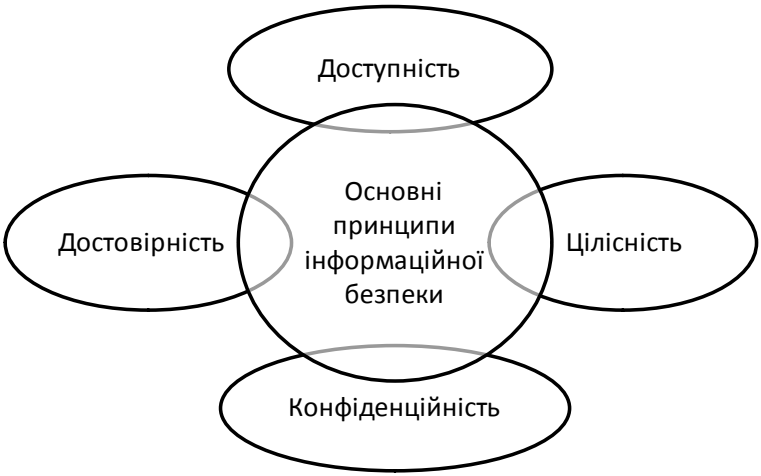


Рис. 1.6. Основні принципи інформаційної безпеки

Доступність інформаційних ресурсів – це можливість за прийнятний час одержати необхідну інформаційну послугу, яка знаходиться у вільному доступі. Інформація повинна надаватися повноправним користувачам ресурсів своєчасно й безперешкодно. Тому, не протиставляючи доступність решті аспектів, її можна виділити як найважливіший елемент інформаційної безпеки.

Цілісність інформаційних даних означає здатність інформації зберігати початковий вигляд і структуру як у процесі зберігання, так і після неодноразової передачі. Вносити зміни, видаляти або доповнювати інформацію вправі тільки власник або користувач із легальним доступом до даних. Цілісність виявляється найважливішим аспектом ІБ у тих випадках, коли інформація служить «керівництвом до дії».

Конфіденційність – це захист від несанкціонованого доступу до інформації. У процесі дій і операцій інформація стає доступною тільки користувачам, які включені до інформаційної системи й успішно пройшли ідентифікацію.

Достовірність указує на приналежність інформації довіреній особі або власнику, який одночасно виступає в ролі джерела інформації, це гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор. Достовірність інформації безпосередньо впливає на суспільну та індивідуальну свідомість, такою ж мірою й на громадську думку, і в силу цього стає одним із основних принципів забезпечення інформаційної безпеки [37].

Власне, у контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки існують 8 факторів (об'єктивні та суб'єктивні) (рис. 1.7.) [30,31].

До інтелектуального (психологічного) фактору можна віднести такі характеристики української суспільної свідомості та явища негативного характеру, що в сукупності гальмують процеси інформаційного розвитку суспільства та забезпечення інформаційної безпеки: ірраціональність, консерватизм та апатичність суспільної свідомості; відсутність сформованості в загальносуспільній свідомості інформаційних потреб; відсутність усвідомленості інформаційних загроз; низький рівень правової свідомості громадян; падіння рівня загальної освіти й культури громадян; загальна поширеність правового нігілізму.

Ускладнює процеси утворення інформаційного права на всіх його етапах формування, формулювання на етапі реалізації права. Стрімка динамічність інформаційної сфери потребує своєчасного розвитку законодавчої бази держави.

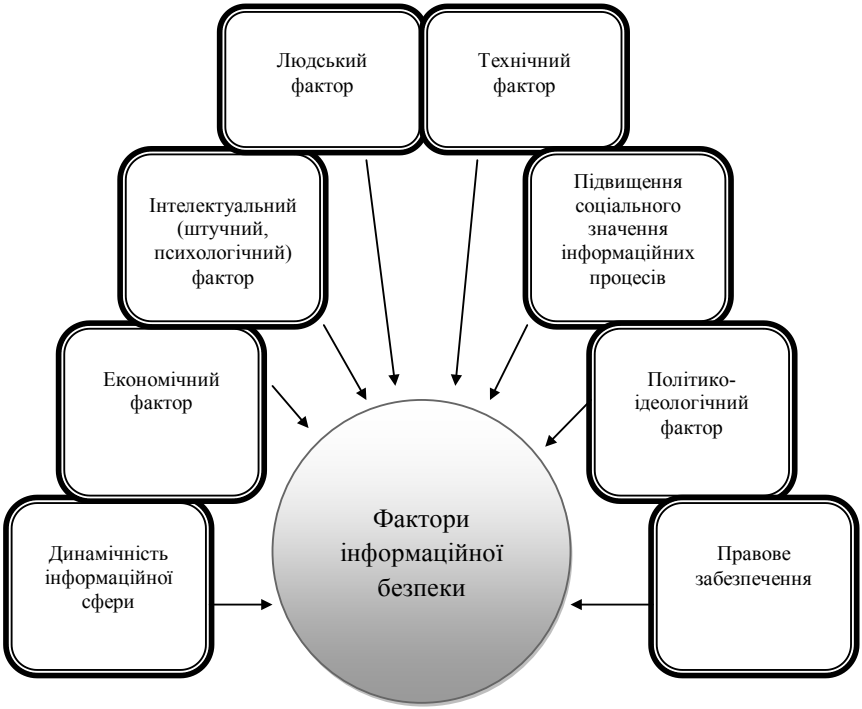


Рис. 1.7. Фактори інформаційної безпеки

Основні чинники динамічності перетворень в інформаційній сфері: стрімкий розвиток інформаційної сфери та інформаційно-комунікаційних технологій; підвищена складність і різноманітність суспільних відносин в інформаційній сфері; новизна інформаційних відносин та відсутність досвіду їх правового регулювання; відсутність в інформаційній сфері загальноприйнятих варіантів поведінки, вироблених суспільством [38].

Шульга В.І. визначає підвищення соціального значення інформаційних процесів [39], як пріоритетність організаційно-забезпечувальної діяльності держави в інформаційній сфері, як

основу подальшого розвитку суспільства, що підтверджується такими чинниками: усепроникливість інформаційних процесів; створення широких інформаційно-комунікативних можливостей; виникнення додаткових можливостей саморозвитку суб'єктів; виникнення нових особливо небезпечних загроз суспільній безпеці; безпрецедентне підвищення загально соціального значення всіх складових інформаційної безпеки. Економічний фактор створює економічне підґрунтя інформаційного розвитку суспільства й держави та матеріально-технічні можливості впровадження інформаційно-комунікаційних технологій. Узагальнені чинники економічного характеру, що визначають результативність процесу забезпечення інформаційної безпеки: відсутність стабільного зростання економіки; низький рівень забезпеченості широких верств населення всіма необхідними для розвитку матеріально-технічними засобами; низький рівень забезпеченості апарату держави сучасними інформаційно-комунікаційними засобами; недостатність фінансування сфери освіти та науки.

Складові технічного фактору характеризують технічну досконалість і сучасність засобів обробки інформації, що визначає рівень технічної готовності до розгортання інформаційних процесів. Основні з них: нерозвиненість мережі швидкісного Інтернету; недосконалість інформаційних ресурсів; застарілість автоматизованих систем обробки інформації.

Політико-ідеологічний фактор визначає рівень усвідомленості соціально сильними групами індивідів необхідності вирішення соціальних проблем та проблем інформаційної сфери. Як вважає Ковтун С.В. [30], до нього можна віднести відсутність сталої, незалежної від політичних персон, стратегії становлення України на світовій арені; відсутність реальної, послідовної та виваженої державної програми соціального розвитку; неправовий характер діяльності державної влади; пріоритетність політичної доцільності над правовою; бюрократичність апарату держави; нерозвиненість громадянського суспільства; нероз-

виненість інформаційних зв'язків між державою й суспільством тощо.

Із точки зору Тихомирова О. [32], інформаційна безпека виступає об'єктом правового захисту. Правові засоби забезпечення інформаційної безпеки є провідним фактором захисту національних інтересів у цій сфері, а їхнє застосування визначається оптимізацією балансу відносин між правом суб'єктів інформаційних відносин на отримання інформації та правом на встановлення обмежень таких відносин із боку інших осіб щодо відомостей, володарями яких вони є; розробкою та реалізацією правових заходів захисту інформації, доступ до якої повинен обмежуватися правовими підставами в процесі захисту інформаційних ресурсів. Правове забезпечення ліквідації загроз і ризиків у сфері інформаційної безпеки є основним фактором структурування, формування, розглядається як законотворча діяльність, що спрямована на запобігання шкоди інтересам особи, суспільства та держави в інформаційній сфері.

Людський фактор заслуговує особливої уваги на думку багатьох авторів, у тому числі Маркова Д.Г. [33], тому що саме люди формують режим інформаційної безпеки і вони ж виявляються головною загрозою. Слід усвідомити той ступінь залежності від комп'ютерної обробки даних, до якого потрапило сучасне суспільство. Оскільки людина є споживачем інформації та суб'єктом її обробки, завжди існував, існує й буде існувати ризик, пов'язаний із помилкою у прийнятті рішення.

Одним із пріоритетних завдань держави на етапі розвитку є визначення напрямків правового регулювання та створення правових гарантій, необхідних для самореалізації суб'єктів в інформаційній сфері. Більшість із перелічених факторів є загальними чинниками (джерелами) процесу утворення національного права і тому дозволяють розглядати процеси розвитку інформаційного права України в контексті проблем становлення правової системи України в цілому.

Підсумовуючи, зазначимо, що сутність інформаційної безпеки держави можна визначити як стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу.

Інформаційна (інформаційно-психологічна) безпека особистості в сучасному суспільстві постає як нагальна проблема, що потребує комплексного та системного вирішення. Суспільно значущі фактори державної інформаційної безпеки зумовлюють особливу важливість та пріоритетність різнопланової високопрофесійної державної діяльності в інформаційній сфері, юридичного її забезпечення, а також виваженого вибору методів правового регулювання.

1.5. Інформаційна безпека як складова національної безпеки держави

У сучасному світі все більше зростає роль інформаційної сфери життя суспільства, яка розглядається як сукупність інформації, інформаційної інфраструктури, суб'єктів інформаційних правовідносин та системи регулювання суспільних відносин, що виникають при цьому. У свою чергу, інформаційна сфера має дуже істотний вплив на стан політичної, економічної, оборонної та інших складових безпеки держави. Тобто, національна безпека залежить від забезпечення інформаційної безпеки, і з подальшим розвитком у сфері інформаційних технологій ця взаємозалежність буде тільки зростати та набувати більшого значення для держави та суспільства в цілому. Так, у ст.17 Конституції України зазначено, що інформаційна безпека є найважливішою функцією держави, справою всього Українського народу [40].

Із розвитком інформаційних технологій і інформаційного суспільства, в умовах глобалізації виникло ціле коло невирішених питань і проблем, істотно змінилась характеристика викли-

ків і загроз цивілізації. Головні цінності, для захисту яких держави прагнуть сформувати ефективні механізми протидії викликам і загрозам, – світ, безпека, права людини і стійкий розвиток держави [41, 42].

Стосовно дослідження проблем державної безпеки, то у своїх працях науковці розглядають їх шляхом комплексного підходу відносно світового та вітчизняного досвіду її забезпечення. Наприклад, Кормич Б.А., визначає інформаційну безпеку як стан захищеності параметрів інформаційних процесів, відносин і норм, які встановлені законодавством. Це забезпечує необхідні умови існування суспільства, держави, людини як суб'єктів таких процесів та відносин [43]. Лопатін В.М. стверджує, що інформаційна безпека є станом захищеності життєво важливих інтересів держави, суспільства та особи на збалансованій основі, тобто національних інтересів країни, від внутрішніх і зовнішніх загроз в інформаційній сфері [44].

Український учений Баранов О. визнає інформаційну безпеку як стан захищеності національних інтересів країни в інформаційному середовищі. За таких умов зводиться до мінімуму чи не допускається взагалі заподіяння шкоди державі, суспільству чи особі через несанкціоноване поширення інформації, її недостовірність, несвоєчасність, через негативні наслідки функціонування інформаційних технологій чи негативний інформаційний вплив [45]. Як показує аналіз наукової літератури, інформаційна безпека є складовою частиною національної безпеки держави, а процес забезпечення інформаційної безпеки необхідно розуміти як «…одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління» [39].

Згідно із Законом України «Про Концепцію Національної програми інформатизації», інформаційна безпека є невід'ємною складовою оборонної, економічної, політичної, а також інших складових національної безпеки [46], вона є станом за-

хищеності життєво важливих інтересів особи, суспільства й держави від внутрішніх і зовнішніх загроз. Отже, національна безпека залежна від змісту національно-державних інтересів та характеризує положення країни, при якому їй не загрожує небезпека війни або інших посягань на суверенний розвиток.

Національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [47]. Основними компонентами національної безпеки є військова, економічна, соціальна, екологічна, інформаційна безпека (рис. 1.8.).

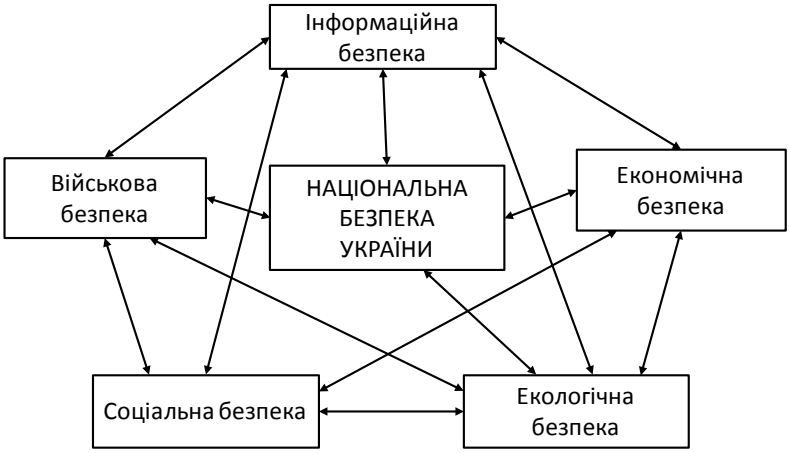


Рис. 1.8. Основні компоненти національної безпеки України

Сама по собі національна безпека представляє геополітичний аспект безпеки взагалі, увесь комплекс питань фізичного виживання держави, захисту і збереження його суверенітету й територіальної цілісності, що охоплює. На сьогодні проблема інформаційної безпеки є дуже важливою, оскільки значно зросла роль накопичення, обробки й поширення інформації, зокрема, в ухваленні стратегічних рішень, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Ін-

формація грає все більшу роль у процесі життєдіяльності людини.

У загальному значенні безпека – це стан захищеності від чого завгодно та може застосовуватися як щодо особистості зокрема, так і суспільства та держави в цілому. Водночас, безпека як поняття, відрізняється в залежності від сфери застосування: політології, соціології економіки і т.ін. У теорії національної безпеки широко використовуються такі формулювання: «національна безпека», «безпека особистості», «державна безпека», «міжнародна безпека», «інформаційна безпека», «політична безпека», «соціальна безпека», «військова безпека» та ін. [24, 48, 49].

Щодо визначення поняття «інформаційна безпека» на сьогодні відсутній цілісний підхід, і єдиної думки щодо її визначення серед дослідників не існує. 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 [25, 34, 50].

Олійником О.В. [51] змістове наповнення поняття «інформаційна безпека» визначається трьома складовими: задоволенням інформаційних потреб суб'єктів в інформаційному середовищі, безпекою інформації, захистом суб'єктів інформаційних відносин від негативного інформаційного впливу (рис. 1.9.).

Перша складова	Друга складова	Третя складова
• задоволення інформаційних потреб суб'єктів в інформаційному середовищі	• безпека інформації	• захист суб'єктів інформаційних відносин від негативного інформаційного впливу

Рис. 1.9. Складові поняття «інформаційна безпека»

Перша – задоволення інформаційних потреб суб'єктів в інформаційному середовищі. Очевидно, що без наявності в суб'єкта необхідної інформації не може бути забезпечена інформаційна безпека. Інформаційні потреби різних суб'єктів не однакові, однак у будь-якому випадку відсутність необхідної інформації може мати негативні наслідки.

Друга – безпека інформації. Вимоги повноти, достовірності та своєчасності інформації повинні дотримуватися протягом усього часу циркуляції інформації, оскільки їх порушення може призвести до невірних рішень або взагалі до неможливості прийняття рішень, як і порушення статусу конфіденційності може знецінити інформацію. Тому інформація повинна бути захищена від впливів, що порушують її статус.

Третя – захист суб'єктів інформаційних відносин від негативного інформаційного впливу. До прийняття невірних рішень може призвести не тільки відсутність необхідної інформації, але й наявність шкідливої, небезпечної для суб'єкта інформації, яка найчастіше цілеспрямовано нав'язується;

При такому підході можна сформулювати наступне визначення: *інформаційна безпека – стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу.* У даному визначенні суб'єктами інформаційних відносин можуть бути держава, суспільство, організації, людина.

У контексті національної безпеки більш повним визначенням інформаційної безпеки можна вважати наступне: *«інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства й держави, при якому зводиться до мінімуму завдання шкоди через неповноту, невчасність та невірогідність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації» [52].*

Спираючись на дані визначення, можна виділити три основні напрямки забезпечення інформаційної безпеки:

– захист інформаційних прав і свобод людини і громадянина;

– захист інформаційних ресурсів, у тому числі й інформації з обмеженим доступом, від неправомірного доступу;

– захист суспільства від шкідливої і недоброякісної інформації.

У свою чергу, небезпечні інформаційні дії зазвичай розділяють на два види. Перший пов'язаний зі втратою цінної інформації, що або знижує ефективність власної діяльності, або підвищує ефективність діяльності супротивника, конкурента. Якщо об'єктом такої дії є свідомість людей, то йдеться про розголошування державних таємниць, вербування агентів, спеціальні заходи й засоби для прослуховування, використання детекторів брехні, медикаментозних, хімічних, інших діях на психіку людини. Безпеку від інформаційної дії цього виду забезпечують органи цензури, контррозвідки й інші суб'єкти інформаційної безпеки. Якщо ж джерелом інформації служать технічні системи, то йдеться вже про технічну розвідку, або шпигунство (перехоплення телефонних розмов, радіограм, сигналів інших систем комунікації), проникнення до комп'ютерних мереж, банків даних.

Другий вид інформаційної дії пов'язаний зі впровадженням негативної інформації, що може не лише призвести до небезпечних помилкових рішень, але і змусити шкідливо діяти, навіть підвести суспільство до катастрофи. Інформаційну безпеку цього виду повинні забезпечувати спеціальні структури інформаційно-технічної боротьби. Вони нейтралізують акції дезінформації, притинають маніпулювання громадською думкою, ліквідують наслідки комп'ютерних атак. Розвиток і впровадження в різні сфери життя суспільства нових інформаційних технологій, як і будь-яких інших науково-технічних досягнень, не лише забезпечують комфортність, але й нерідко несуть небезпеку.

Визначимо найбільш суттєві *групи інформаційно-технічних небезпек*. *Перша* група пов'язана з бурхливим розвитком нового класу зброї – інформаційної, що здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства. У відносно мирних умовах інформаційно-психологічні технології можуть застосовуватися в якості спеціальних механізмів управління кризами і провокації жорстокості на території супротивника. *Друга* група інформаційно-технічних небезпек для особи, суспільства й держави – це новий клас соціальних злочинів, що ґрунтуються на використанні сучасних інформаційних технологій (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Питання забезпечення інформаційної безпеки як однієї із важливих складових національної безпеки держави особливо гостро постає в контексті появи транснаціональної трансграничної комп'ютерної злочинності й кібертероризма. *Третя* група інформаційних небезпек– використання нових інформаційних технологій у політичних цілях.

Складності у сфері державного регулювання інформаційною безпекою: на сьогодні відсутня чітко виражена організована система вироблення та реалізації єдиної державної політики у сфері забезпечення інформаційної безпеки, що займається визначенням пріоритетів розвитку єдиного інформаційного простору. Спираючись на це, необхідно визначити причини, що зумовлюють незадовільний стан у сфері забезпечення інформаційної безпеки, серед яких:

– безсистемний розвиток законодавства, що регулює інформаційну сферу;

– низький рівень правової та інформаційної культури громадян і суспільства в цілому;

– незадовільне фінансування діяльності забезпечення інформаційної безпеки;

– недостатній розвиток інформаційних і комунікаційних технологій в області державного управління, неготовність ор-

ганів державної влади до застосування ефективних технологій управління й організації взаємодії з громадянами і господарюючими суб'єктами;

– недостатній рівень підготовки кадрів в області створення і використання інформаційних і комунікаційних технологій.

Державне врегулювання безпеки, а саме регламентація основних принципів і зміст діяльності щодо її забезпечення приведені в Законі України «Про національну безпеку» від 21.06.2018 року № 2469-VIII. Цим законом визначається та розмежовуються повноваження державних органів у сферах національної безпеки й оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки й оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки й оборони, забезпечуючи в такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки й оборони [47].

Основні принципи забезпечення безпеки: дотримання й захист прав і свобод людини і громадянина; законність; системність і комплексність застосування публічними органами влади політичних, організаційних, соціально-економічних, інформаційних, правових та інших заходів забезпечення безпеки; пріоритет запобіжних заходів у цілях забезпечення безпеки; взаємодія органів державної влади із громадськими об'єднаннями, міжнародними організаціями і громадянами в цілях забезпечення безпеки.

Діяльність держави щодо забезпечення безпеки включає:

1) прогнозування, виявлення, аналіз і оцінку загроз безпеки;

2) визначення основних напрямків державної політики і стратегічне планування в області забезпечення безпеки;

3) правове регулювання в області забезпечення безпеки;

4) розробку й застосування комплексу оперативних і довготривалих заходів з виявлення, попередження і усунення загроз безпеки, локалізації і нейтралізації наслідків їх прояву;

5) застосування спеціальних економічних заходів у цілях забезпечення безпеки;

6) розробку, виробництво і впровадження сучасного вигляду озброєння, військової і спеціальної техніки, а також техніки подвійного й цивільного призначення в цілях забезпечення безпеки;

7) організацію наукової діяльності в області забезпечення безпеки;

8) координацію діяльності регіональних органів державної влади, органів державної влади суб'єктів України, органів місцевого самоврядування в області забезпечення безпеки;

9) фінансування витрат на забезпечення безпеки, контроль за цільовим витрачанням виділених засобів;

10) міжнародна співпраця в цілях забезпечення безпеки;

11) здійснення інших заходів в області забезпечення безпеки відповідно до законодавства України.

Так, у Законі України «Про національну програму інформатизації» визначається, що головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [53].

Таким чином, із вищезазначеного можна зробити висновок, що «безпека» розглядається як поняття, що відображає стан об'єкта в системі його зв'язків із точки зору здатності самовиживання в умовах внутрішніх та зовнішніх загроз, а також в умовах дій непередбачених та тяжко прогнозованих факторів. Національна безпека України складається із сукупності складових, які повинні забезпечувати збалансовані інтереси особи, суспільства й держави. До цих складових відносяться безпека

в міжнародній економічній, військовій, внутрішньополітичній, інформаційній, соціальній, екологічній і інших сферах. При цьому, як уже зазначалося, одна з ключових ролей у системі забезпечення національної безпеки відводиться економічній та інформаційній складовим.

Базовим документом, що визначає зміст національних інтересів України в інформаційній сфері, є Доктрина інформаційної безпеки України. Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки й оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Стратегія національної безпеки України є обов'язковим для виконання документом і основою для розробки конкретних програм за складовими державної політики національної безпеки [54].

У Доктрині інформаційної безпеки закріплені наступні актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення й дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах із метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Національна безпека нерозривно пов'язана з діяльністю держави. Тільки вона, спираючись на свій апарат, владні органи, діяльність яких поставлена в жорсткі рамки і підкріплюється відповідними правовими актами, може забезпечити спокій громадян, створити сприятливі умови для їхнього життя та діяльності. Ніякі інші соціальні сили не зможуть виконати цього завдання. Забезпечення власної безпеки та своїх громадян є одним із основних завдань будь-якої держави. Успішний розвиток і саме існування України як суверенної держави неможливі без забезпечення її національної інформаційної безпеки.

У світі розвитку інформатизації і глобалізації роль інформаційної безпеки особи, суспільства, держави збільшується, і її забезпечення повинно зайняти належне місце в політиці держави. Виходячи з цього, зазначимо основні завдання, що вимагають вирішення в забезпеченні інформаційної безпеки як складової національної безпеки держави:

1. Необхідність нормативно-правового регулювання щодо протидії використання інформаційних технологій, які загрожують інтересам держави;

2. Необхідність створення економічних передумов для розвитку національних інформаційних ресурсів та інфраструктури, впровадження новітніх технологій в інформаційну сферу;

3. Необхідність удосконалення виробництва вітчизняних інформаційних технологій, що розробляються, впровадження вітчизняних розробок, підвищення ефективності наукових досліджень та якості освіти у сфері інформаційних технологій.

Інформація стала одним із чинників, здатних призвести до великомасштабних аварій, військових конфліктів і дезорганізації державного управління. І чим вищий рівень інтелектуалізації й інформатизації суспільства, тим надійніша його інформаційна безпека. Тому Україні необхідно приділяти своїй національній інформаційній безпеці особливу увагу, оскільки вона є основою визначення найважливіших напрямків і принципів державної політики країни, життєво важливих інтересів особи, держави і суспільства.

Список використаних джерел

1. Гринберг Р. С. Основные проблемы современного турбулентного мира. Гуманитарий Юга России. 2013. № 2. С. 22-28.

2. Резеньков Д.Н., Приходько С.С. Понятие «социальная турбулентность» в современном мире в концепции информационной безопасности России. Культура и общество: история и современность. Материалы II Всероссийской (с международным участием) научно-практической конференции. Под редакцией Колосовой О.Ю, Гударенко Р.Ф., Ряснянской Н.А, Красиковой Е.А. Ставрополь. Издательство ООО «Ветеран». 2013. С. 128-130.

3. Щекотин Е.В. Социальное управление в турбулентном обществе: вопросы безопасности и риска. Социум и власть. 2016. № 1 (57). С. 87-92.

4. Щекотин Е.В. Проблема благополучия в турбулентном социуме: аспект безопасности. Вестник науки Сибири. 2017. №4 (27). С. 74-83.

5. Чудинов С.И., Щекотин Е.В. Турбулентный социум и концепция безопасности: социально-философские аспекты: монография. Новосибирск: Изд-во НГТУ. 2018. 159 с.

6. Панченко О.А. Информационно-психологическая безопасность в эпоху турбулентности: монография. К.: КВИЦ. 2020. 480 с.

7. Розов Н.С. Эпохи турбулентности и их преодоление. Полития. № 1 (92). 2019. С. 81-96.

8. Яницкий О.Н. Социология критических состояний общества: теоретические и методические проблемы. Социологическая наука и социальная практика. 2014. №4(8). С. 5-24.

9. Панченко О.А. Турбулентні соціально-психологічні виклики в системі державного управління інформаційною безпекою. Теорія та практика державного управління. 2020. Том 1. № 68. С. 210-217.

10. Arsenalt A. and Castells M. Switching Power: Rupert Murdoch and the Global Business Media of Media Politics. International Sociology. 2008. №23 (4). P. 488-513.

11. Social Turbulence and Governmental Form. 2016. URL:https://neociceroniantimes.wordpress.com/2016/11/09/social-turbulence-and-governmental-form/ (дата звернення: 23.05.2019).

12. Даниэль Эстулин. Тавистокский институт (перевод П. Смирнов). Минск, 2014. URL: http://coollib.com/b/284081(дата звернення: 28.01.2020).

13. Буданов В.Г. Метаморфозы социальной реальности эпохи перемен: онтологии и технологии. Творческие поиски ученых Израиля и мира сегодня. Сборник статей. Международный центр научных исследований и практики творчества. Израиль – Ашкелон. 2013. С.68-74.

14. Елагин А.Г. Потребность человека быть в безопасности. Пробелы в российском законодательстве. 2016. № 3. С. 11-13.

15. Рашидова С.С. Визначення феномену і поняття «потреба». Духовність особистості: методологія, теорія і практика. 2015. № 5 (68). С. 106-121.

16. Мамонов І., Потреби та інтереси людини як основа публічного управління. Вісник Національної академії державного управління при Президентові України. 2012. Вип. 3. С. 212-220.

17. Панченко О.А. Інформаційна безпека держави як елемент соціальної культури. Аспекти публічного управління. 2020. № 1. Том 8. С. 58-67.

18. Панченко О.А. Суспільний запит на інформаційну безпеку. Публічне урядування. 2020. № 2 (22). С. 141-149. DOI: 10.32689/2617-2224-2020-2(22)-141-149.

19. Хромченко А.Л. К вопросу о разработке классификации потребностей в российской научной традиции. Общественные науки и современность. 2007. № 4. С. 144.

20. Маслоу А.Г. Мотивация и личность. 3-е. изд. СПб.: Питер, 2008. 357 с.

21. Панченко О.А., Кабанцева А.В., Сердюк І.А. Потреби особистості на інформаційну безпеку. Публічне урядування. 2020. № 3 (23). С. 203-214. DOI: https://doi.org/10.32689/2617-2224-2020-3(23)-203-214.

22. Мрочко Л.В., Пирогов А.И. Информационные потребности и интересы личности: связь и соподчинение общего и частного. Экономические и социально-гуманитарные исследования. 2016. № 3 (11). С. 125-129.

23. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки. Вип. 2. № 1. 2016. С. 27–32.

24. Марущак А.І. Дослідження проблем інформаційної безпеки у юридичній науці. Правова інформатика. 2010. № 3(27). С. 17–21.

25. Лисовская Ю.П. Информационная безопасность в современном глобализованном мире. Веснік БДУ. 2015. № 2. С. 93–97.

26. Овчаров А. Вплив соціально-психологічних технологій на соціальне середовище. Соціальна психологія. 2008. № 6. С. 34–42.

27. Петрухно Ю.Є. Інформаційне суспільство: поняття, основні складові, характеристика. Вісник ОНУ. 2014. Т. 19, вип. 1. С. 127–133.

28. Клейберг Ю.А. Десоциализация и дегуманизация личности в ситуации социальной турбулентности: психолого-девиантологический дискурс. Вестник краснодарского университета МВД России. 2017. № 1(35). С. 150–158.

29. Панченко О.А, Сердюк І.А. Роль держави в особистісних та суспільних відносинах в епоху турбулентності. Материалы Международной научно-практической интернет-конференции «Тенденции и перспективы развития науки и образования в условиях глобализации». (28 февраля 2020 г.) Переяслав – 2020. Вып. 56. С. 42-45.

30. Ковтун С.В. Інформаційна безпека: підручник. Харків. Вид. ХНЕУ, 2009. 368 с.

31. Кустовська О.В. Методологія системного підходу та наукових досліджень: Курс лекцій. Тернопіль: Економічна думка, 2005. 124 с.

32. Тихомиров О. Забезпечення інформаційної безпеки: теоретико-правовий аспект. Право України. 2011. № 4. С. 252–259.

33. Маркова Д.Г. Человеческий фактор в информационной безопасности. Известия ТулГУ. Технические науки. 2018. Вып. 10. С. 149–152.

34. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. Науковий вісник. Серія «Філософія». Харків: ХНПУ. 2017. Вип.48 (частина І). С. 212-219.

35. Перун Т.С. Принципи забезпечення інформаційної безпеки України в умовах євроінтеграції. Eurasian Academic Research Journal. 2017. № 11 (17). С. 108–114.

36. Муравська (Якубівська) Ю.Є. Інформаційна безпека суспільства: концептуальний аналіз. Економіка і суспільство. 2017. Вип. № 9. С. 289-294.

37. Довнар Н.Н. Достоверность информации как фактор обеспечения информационной безопасности. Вестник ЮУрГУ. Серия «Право». 2015. Т. 15, № 1. С. 57–62.

38. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика» 2017. 168 с.

39. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514. (дата звернення: 23.05.2019).

40. Конституція України. Закон від 28.06.1996 № 254к/96-ВР. – Редакція від 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show /254%D0%BA/96-%D0%B2%D1%80.

41. Губенков А.А., Байбурин В.Б. Информационная безопасность. М.: «Новый издательский дом». 2005. 128 с.

42. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 25.00.02 «Механізми державного управління». В.І. Гурковський. Київ. 2004. URL: http://otherreferats.allbest.ru/law/00440507_0.html. (дата звернення: 23.05.2019).

43. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса: Юридична література. 2003. 472 с.

44. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. СПб.: Фонд «Университет». 2000. 428 с.

45. Баранов А. Информационный суверенитет или информационная безопасность? Нац. безпека і оборона. 2001. № 1(13). С. 70-76.

46. Закон України «Про Концепцію Національної програми інформатизації». Концепція від 04.02.1998 № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80. (дата звернення: 23.05.2019).

47. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2469-19. (дата звернення: 23.05.2019).

48. Форос Г.В., Жогов В.С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. Правова держава. 2019. № 33. С. 128–134.

49. Почепцов Г.Г. Інформаційна політика: навчальний посібник. К.: Вид-во УАДУ, 2002. 88 с.

50. Триняк В.Ю. Сутнісні аспекти інформаційної безпеки в умовах глобалізації. Наукові записки Харківського університету Повітряних Сил. Соціальна філософія, психологія. Харків: ХУПС. 2007. Вип. 3 (29). С. 142–149.

51. Олійник О.В. Адміністративно-правові засади інформаційної безпеки. Європейські перспективи. 2012. № 4 (1). С. 65-68.

52. Панченко О.А. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. Серія: Державне управління. 2019. Випуск 3. URL: http://77.222.145.174/index.php/governance/article/view/296/297. (дата звернення: 23.05.2019).

53. Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР. URL: https://zakon.rada.gov.ua/ laws/show/74/98-%D0%B2%D1%80 (дата звернення: 23.05.2019).

54. Указ президента України №47/2017.Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення: 28.02.2017).

РОЗДІЛ 2

Стан державного управління в умовах суспільно-інформаційної турбулентності

2.1. Турбулентні явища та суспільні метаморфози як фактори ризиків державного управління

Поняття «турбулентність» досліджувалось із точки зору інформаційно-психологічної безпеки особистості ([1-5]). При цьому взята за основу така інтерпретація турбулентності: безладні завихрення енергетичних потоків. Турбулентність виникає при зустрічі із протилежним потоком, або з перешкодою. Із цього визначення можна вибрати такі «соціальні характеристики»: рух (потік), безлад (нестійкість), зміна стану речей. З останньою характеристикою асоціюється й поняття «метаморфоза» (докорінна зміна, перетворення). Яницький О.Н., наприклад, дає таке визначення: «Турбулентність насправді означає крайній ступінь нестабільності світової економічної і політичної системи, коли ймовірність досягнення точки її біфуркації і/або злому дуже висока» [6]. Виникнення критичної точки турбулентності пов'язане з низкою тенденцій сучасного світового розвитку, що супроводжується незворотними радикальними змінами – метаморфозами. Виникає замкнуте коло, коли одне породжує інше і навпаки. Для підтвердження цього нами виділено п'ять найбільш вагомих аргументів [7].

По-перше, суспільство, яке змінюється, є перманентним генератором метаморфоз. Інновації можуть бути настільки відмінні від попередніх реалій, що сприймаються людьми як шок. Джерелом збудження як причини турбулентності є, у першу чергу, протистояння еліт у боротьбі за владу й політична «незадоволеність» населення. Особливо яскраво цей процес спостерігається під час виборів і зміни правлячих еліт. І саме держави з демократичною формою правління, яким властиві свобода

слова і плюралізм, найбільш уразливі в плані виникнення турбулентності.

По-друге, турбулентні явища, пов'язані з глобалізацією та періодичними економічними кризами, докорінно змінюють світ. В умовах глобалізації він не став більш стабільним і передбачуваним. Навпаки, його головними характеристиками стали хаос і підвищений потенціал конфліктності. Поки економіка розвивається, настрій у суспільстві в цілому позитивний. Але під час кризи, коли життєві стандарти різко знижуються, виникає різке невдоволення населення. І навіть розвиваючись, світова економіка, нерівномірно розподіляє продукт свого розвитку. Багато держав, регіонів, перебуваючи на «периферії», живуть на дотації «центру» або позикові кошти. Нерівномірно розподілений фінансовий капітал спричиняє переміщення робочої сили (у тому числі й нелегальної), матеріалів, енергії. У таких умовах сталий розвиток стає більш ніж проблемним.

Глобалізація також породила метаморфози відкритості і закритості соціуму. Раніше традиційне суспільство відрізнялося своїми «жорсткими» цінностями й нормами, які підтримувалися завдяки політичним і культурним межам. Ідеологи лібералізму розглядають відкритість кордонів соціуму як «універсальний» ідеал для всього людства. Однак його реалізація (на прикладі біженців) стала сьогодні шоком для багатьох європейців. Слід зазначити, що турбулентність генерується самим фактом різноманітності культур і життєвого укладу. Масове ж «нашестя» чужорідних культур вимагає від Європи все більших зусиль із підтримки «єдності в різноманітті» для запобігання міжнаціональним конфліктам.

Як це не парадоксально, в умовах відкритості виникають метаморфози закритості у вигляді небачених раніше локальних сегрегацій і анклавних спільнот. За одним зі сценаріїв розвитку суспільства в умовах турбулентності, це його сегментація, коли кожна група (етнічна, расова, гендерна) воює проти всіх інших. Нації розпадаються на регіональні групи, які, у свою чергу, дро-

бляться на ще більш дрібні етнічні групи заради спрощення процесу прийняття рішень. Природні лінії поділу суспільства перетворюються на барикади. Приклад – світова турбулентність у вигляді коронавірусу COVID-19, унаслідок якого Євросоюз фактично опинився в стані паралічу. Причина навіть не в тому, що були закриті кордони його держав-членів, а в тому, що кожна держава відособилась у своїх проблемах. І коли в Італії розпочався дефіцит медичних масок, апаратів штучного дихання, тестів на вірус та іншого обладнання, вона не змогла закупити необхідне в інших країнах Євросоюзу. Держави закриваються й можуть розраховувати тільки на власне виробництво та зайнятість населення всередині держави.

Розмірковуючи про некеровану відкритість, мусимо зазначити, що вона виробляє і небезпечні для соціуму метаморфози в духовному житті, які виражені в зростаючому символічному насильстві, обумовленому комерціалізацією мас-медіа: сенсаційність, фейкові новини підмінили собою якісну аналітичну інформацію й мистецтво, а шоумейкери буквально витіснили з екранів освітні програми, затьмарили цінності сім'ї, навчання, праці. Це викликає соціальну тривогу й невизначеність.

По-третє, зміна взаємовідносин між людством і біосферою призвела до появи складних соціальних і техноприродніх гібридів, як правило, глобального характеру. До недавнього часу людина вважала себе господарем природи. Однак на сьогодні все більше свідчень того, що Біосфера (через природні аномалії і катастрофи) усе частіше визначає поведінку людини й соціуму. Панування над природою змінюється проблемою збереження того, що людині вдалося досягти. Це підтверджує і О.Н. Яницький, коли говорить, що звичний поділ на природу й суспільство більше не відповідає процесам стиснення й інтеграції всього того, що відбувається на Землі [8]. Ми тепер живемо в соціобіотехносфері, її закони нами ще не досліджені. По суті, стався ряд метаморфоз із природою, соціумом, технічними новаціями, які раніше представляли самостійну реальність, а нині в багатьох

випадках утворюють єдине ціле. Одним із таких гібридів є вже наведений приклад пандемії коронавірусу COVID-19, яка струснула планету останнім часом.

По-четверте, турбулентні світові тенденції відображають небезпечний характер розвитку подій, який характеризується метаморфозою стирання роздільних ліній між станом війни і миру. Конкуруючі між собою сторони все частіше вдаються не до правових вирішень спорів, а до інших засобів, що дозволяє комплексно впливати на розвиток кризової ситуації у своїх інтересах і при цьому створювати видимість неупередженості, приховуючи свою безпосередню задіяність у протистоянні.

Інструменти для досягнення стратегічних цілей, що включають політико-дипломатичні, інформаційно-психологічні, економічні та силові, визначаються як «неявні військові дії», «нелінійні», «асиметричні», «нетрадиційні» та «гібридні» операції. Узагальненим поняттям для позначення нової форми протиборства стало «гібридна війна – приховані агресивні дії, що йдуть урозріз із нормами міжнародного права» [9].

Політика явного примусу силою до цих пір існує, змінилися тільки її форми та інструменти. Ще більше турбує те, що політика одностороннього насильства по відношенню до мирних жителів у формі геноциду, тероризму або етнічних чисток, що практикується неурядовими акторами, включаючи «непізнані формування», отримує загальне поширення.

По-п'яте, процес інформатизації світової системи, що сприймається як символ і індикатор прогресу, має декілька проблемних явищ, пов'язаних з інформаційними метаморфозами:

– процес вимагає більшої прозорості інформаційних відносин, а це неминуче призводить до порушення прав і свобод;

– прихід «пост-паперової» культури істотно змінює структуру і функції інститутів управління, освіти і науки;

– загострюється боротьба між глобальними гравцями за роль «програмістів» і «перемикачів» засобів масової інформації

й комунікації, мережевих систем, за допомогою яких формується глобальна політика.

В. Моско вважає, що нині відбувається перехід від постіндустріального й постінтернетного суспільства до суспільства цифрового, побічні ефекти якого змінюють власне людські комунікації на людино-машинні, які, у свою чергу, радикально змінюють природу влади, насильства і справедливості [10]. Останнє ствердження потребує більш детального розгляду.

Метаморфоза соціальної влади в цифрову владу. Влада завжди була соціально обумовленою. Її характер і зміст змінювалися в міру розвитку й ускладнення соціальної структури суспільства. Під впливом прагматичного характеру науки і технологій, інформатизації та діджиталізації соціуму влада радикально змінюється, із неї вихолощується соціальний і культурний контекст. В. Моско підкреслює, що нові реалії цифрового суспільства «фундаментально змінюють стосунки між людьми й цифровими машинами», «означають постійну інтеграцію людей і машин». Але головне, що створюються принципово нові владні структури, «що домінують над цифровим світом», виступають «силою в політико-економічних і геополітичних конфліктах», а також «контролюють індивідуальні тіла й соціальні відносини», беручи на себе функції світового уряду.

Метаморфози соціального насильства в цифрове насильство. У доіндустріальному суспільстві у людей були відносно стійкі уявлення про насильство, які були обумовлені символізацією, життєвим досвідом, культурою. Зараз же в різні форми соціального насильства безпосередньо входять цифрові компоненти, а також побічні ефекти прагматичних трендів розвитку науки і технологій. Найбільші виклики культурі несе саме цифрове насильство. Ми не помітили, як створили міф про те, що діджиталізація представляє тільки блага, незважаючи на весь спектр негативних побічних ефектів даного процесу. У. Вандербург порівнює цифрове насильство з «нашою війною із самим собою» [11]. На його думку, у сучасному суспільстві затвердив-

ся соціальний тип «гомоінформатикус». Тінейджери починають жити так, ніби в них немає культурних ресурсів, відповідно, вони «повинні покладатися на інші численні факти й думки, доступні з їхніх мобільних телефонів, комп'ютерів. Крок за кроком світ стає безпечним для техніки й небезпечним для людей, співтовариств та екосистем».

Цифрове насильство сприяє утвердженню небаченого раніше типу тотального нагляду. Зібрана інформація про користувачів різних сервісів без їхнього відома накопичується в глобальних цифрових структурах. «Повсюдний нагляд збирає стільки даних, скільки можливо, створюючи цифрову версію всевидючого паноптіка усюди вимірюються і відстежуються майже всі аспекти фізичного й ментального функціонування людини».

Метаморфози культурно обумовленої справедливості в цифрову несправедливість. Історично справедливість була обумовлена культурно-локальним контекстом, стосувалася характеру взаємодії людей. Однак нині в уявлення про добро і зло, справедливість і несправедливість включаються технологічні, економічні, цифрові і навіть кліматичні чинники, залишаючи осторонь їхню власну культурну складову.

В уявлення про сучасну справедливість втрутилися економічні міфи про капітал, прогрес, роботу і щастя. Заміщення культурного підходу на економічний поклало початок реорганізації людського життя й суспільства за образом машини, що, по суті, призвело до приниження культурно обумовленої справедливості і становлення цифрової несправедливості. Процеси діджиталізації привнесли нові несправедливості в характер праці, зокрема, роботи не тільки витісняють робочі місця, а й мінімізують культурні зв'язки людей. Нові форми несправедливості проявляються в тому, що «все більше людей працюють як асистенти роботів і інших розумних засобів». Більше того, мозок і мислення людини набувають характеру функціонування цифрової техніки.

Проміжний висновок із наведеного матеріалу полягає в тому, що фундаментальною характеристикою турбулентного соціуму є те, що він допускає існування тільки нестабільних, плинних, мінливих об'єктів. І це є його головною метаморфозою, що стосується також тих соціальних утворень, які є базовими для конструювання життєвого світу людини – державності, сім'ї, праці, власного благополуччя. Хаотичні нелінійні процеси, що мають вирішальний вплив на життя сучасної людини, неможливо редукувати за універсальними правилами. Тут потрібне більш «тонке» налаштування.

Як уже зазначалося, влада завжди була соціально обумовленою. Історично так склалося, що протягом 20-го століття держава брала на себе все більше соціальних обов'язків, «і громадяни тепер чекають від неї найширшого захисту, розв'язання суперечок, виробництва й розподілу». При цьому державою конструюється специфічний об'єкт управління – «населення», благополуччя якого розглядається як статистична категорія, у той час, як питання благополуччя окремої особистості відходить на другий план і переміщується у вузьку область прикладної психології.

Всеохоплюючий процес турбулентності зачіпає й інститути державного управління, послаблюючи їх, що, у свою чергу, прямо впливає на якість життя людей – функції, які держава значною мірою монополізувала, вони перестають виконуватись, у кращому випадку – виконуються неналежним чином. Так, розпад Радянського Союзу, який став соціальною й антропологічною катастрофою, призвів до того, що люди, які знаходились під опікою держави, були покинуті напризволяще. Будучи вихованими й реалізованими в колишньому СРСР, люди вмить опинилися взагалі без нічого – викинуті за борт соціуму, зі збитими орієнтирами, без пошани й поваги, навіть без роботи. Злами стереотипів мислення й поведінки призвели до станів фрустрації: гніву, відчаю, тривоги, роздратування, розчарування і т.ін., або й повної дезорганізації діяльності людини.

Слабкість держави найбільш яскраво виявляється у феномені сучасного тероризму. До недавнього часу механізми забезпечення національної безпеки були спрямовані на боротьбу з ворогом, який явно і стабільно існує в часі й просторі. Сучасний тероризм має зовсім іншу форму. Це мережеві структури, які постійно змінюються, не мають чітких обрисів і кордонів і можуть переходити зі стану ворога в стан союзника і навпаки (приклад – Близький Схід в останні десятиліття). Боротьба з тероризмом, що сприймається як зовнішній ворог, може стати боротьбою держави зі своїми громадянами. По відношенню до такого «потокового» за своєю сутністю явища традиційні інститути, що опікуються безпекою, часто є неефективними, а їхні контртерористичні заходи лише обмежують конституційні права громадян. При цьому вміле й цілеспрямоване маніпулювання тривогами, страхами й розгубленістю простої людини дозволяє сформувати підґрунтя для закриття самого проєкту правової держави.

Одним із альтернативних виходів із ситуації, що склалася, може стати розвиток концепту культури безпеки як «турботи про себе». Спираючись на дослідження Щекотина Є.В. [12,13] у цьому напрямку, відзначимо дві базові складові поняття «культура безпеки»: 1) ціннісно-когнітивна установка – норми, ідеали, повсякденні звички і правила, які регулюють соціальну поведінку людей; 2) сукупність практичних навичок – знання і вміння діяти в ситуації ризикових факторів безпеки (у нашій конкретиці – це «інформаційна культура» та «формування турбулентного мислення»). Поняття «культура безпеки» й «турбота про себе» відображають взаємозалежні явища і процеси. Культура безпеки є категорією психологічною, тому роль людської психіки в забезпеченні безпеки є базовою. Турбота про себе – це характеристика людини та її життєдіяльності, основною передумовою якої є творче освоєння цією людиною культури безпеки. Це означає, що в лінійці ці два поняття включають в себе не лише систему ідеальних уявлень, а й здатність діяти і вести себе

належним чином, тобто є частиною практики конструювання персонального благополуччя. У даному контексті *благополуччя визначається як якісний життєвий стан людини, що вона сприймає, як відчуття щастя.* Таким чином, «турбота про себе» – це набір ціннісних установок, знань, правил і практик, дотримання яких дозволяє особистості жити «щасливим життям», тобто, це шлях досягнення благополуччя.

Як було наголошено, державний підхід до благополуччя наразі заснований на статистичному підході й припущенні, що володіння тим чи іншим благом (матеріальним або нематеріальним) дозволяє судити про ступінь благополуччя людини. Однак в умовах турбулентного соціуму цього недостатньо. Прикладом є ситуація з безпекою. Безпека – одна з основних умов «щасливого життя», і її забезпечення історично є головною функцією держави. Але в сьогоднішніх умовах реалізація цієї функції, по-перше, вступає в протиріччя з іншими складовими «щасливого життя» (наприклад, правом на свободу – переміщення, слова і т.ін.), по-друге, не реалізується на належному рівні (нездатність упоратися з новими викликами, наприклад, із тим же тероризмом).

Щодо шляхів розвитку державної політики й соціального регулювання в умовах турбулентності зазначимо наступне:

Перший напрямок – посилення авторитарних тенденцій державного регулювання. При належному реформуванні, політичній згоді й підтримці суспільства це може спрацювати, але тільки в обмежений часовий проміжок, де наслідком буде скорочення простору вільних можливостей для людини.

Дугий напрямок – послаблення ролі держави, посилення місцевого самоврядування. Ця практика має право на життя, але за умови, що місцеві органи не візьмуть на себе функції «приватної безпеки» і не перетворяться на «окремі князівства», що також загрожує зростанням насильства і свавілля, обмеженням свобод людей. За приклад знову оберемо ситуацію з COVID-19. За благословення держави в областях почали створюватись па-

ралельно до владних, структури у боротьбі із коронавірусом, що призвело до виникнення конфлікту інтересів. Більше того, держава почала підтримувати ці квазізаконні формування, наслідком чого стало суспільне протистояння.

У якості третього варіанта вирішення проблеми може стати симбіоз делегування широких повноважень на локальний рівень при належному контролі центру й «культури безпеки» як форми реалізації турботи про себе. Розвиток цієї практики вимагає зміни підходів до проблеми благополуччя в цілому. Культура безпеки не зводиться до суворого слідування певним наборам правил та інструкцій. Це більш складний процес, який інколи неможливо формалізувати і в якому вирішальну роль відіграють місцеві культуральні спільноти і «локальні» знання, які дозволяють людині найкращим чином пристосуватися до конкретних життєвих умов і нюансів, а також розвиток певних особистісних якостей і компетенцій.

Розвиток культури безпеки передбачає кілька важливих кроків: зміцнення громадянської свідомості, посилення локальних спільнот і розширення певних прав громадян, пов'язаних із самозахистом. Держава має усвідомити необхідність інноваційних заходів, де, перш за все, є відкритість і готовність до сприйняття нових реалій, можливостей, суспільних запитів. У. Бек [14] у посмертно виданій книзі «Метаморфоза сучасного світу» наголошував: «Було б хибно прирівнювати метаморфозу світу зі зміною на краще. Метаморфоза світу нічого не говорить про те, чи є дане перетворення на краще чи на гірше. Як концепція, вона не виражає ні оптимізму, ні песимізму з приводу ходу історії. Вона не описує занепад Заходу, не припускає, що все буде краще. Вона залишає все відкритим і направляє нас до значних політичних рішень». Цей вислів підтверджує нашу думку про те, що суспільство потребує інноваційних політичних рішень, спрямованих на здійснення гуманістичної модернізації, у тому числі сприяння втіленню концепту культури безпеки як «турботи про себе». Зволікання в цьому загрожує глобальними ризиками: ни-

нішні негативні ефекти метаморфоз можуть призвести до переходу фатальної межі як встановленого правопорядку й соціальних відносин, так і умов самого існування суспільства.

Таким чином, можна стверджувати про наявність причино-наслідкового зв'язку між турбулентністю й метаморфозами суспільства. Більше того, це породжує синергетику ризикових явищ щодо суспільних відносин і державного управління. Головною метаморфозою сучасного суспільства є перетворення його в турбулентний стан, де основною ознакою є потокова реальність, і в силу цього суспільство пронизане хаотичними, неконтрольованими процесами. Ці турбулентні явища можуть призвести як до нових революційних змін і відкриття нових можливостей для людини, так і до катастрофічних наслідків. Нестабільне середовище продукує як високі ризики, так і високі шанси для держави не втратити управлінські функції. Важливим завданням є інвентаризація досягнутого, розуміння нових реалій і вироблення відповідної державної політики. Варіантом вирішення проблеми може стати симбіоз делегування широких повноважень на локальний рівень при належному контролі центру й «культури безпеки» як форми реалізації турботи про себе. Розвиток культури безпеки передбачає кілька важливих кроків: це зміцнення громадянської свідомості, посилення локальних спільнот і розширення певних прав громадян, пов'язаних із самозахистом, самоактуалізацією та особистою відповідальністю за теперішнє і майбутнє.

2.2. Соціальні інформаційно-психологічні аспекти в системі державного управління інформаційною безпекою в умовах турбулентності

Як уже було зазначено, сучасний етап світового розвитку характеризується явищами, які отримали назву «турбулентність». Причому турбулентність зачіпає всі сфери людської життєдіяльності, у тому числі й інформаційну, де інформаційне

середовище представляє собою сукупність інформації, інформаційної інфраструктури, соціально-економічних і культурних регуляторів інформаційних процесів [15]. Знаходячись у ІС, суб'єкт інформаційних відносин піддається різним впливам, серед яких: 1) той, що активізує діяльність суб'єкта за рахунок наявності достатньої кількості інформації необхідної якості, тобто високого ступеня задоволення інформаційної потреби; 2) той, що гальмує надмірною кількістю «інформаційних шумів» і низьким рівнем задоволення інформаційної потреби; 3) нейтральний, що не надає суттєвого впливу на діяльність суб'єкта. У цьому полягає суперечливість ІС – поряд із конструктивними впливами, воно володіє й деструктивними. Слово «деструкція» трактується як «порушення, руйнування нормальної структури чого-небудь». Так, деструктивна діяльність людини під дією інформаційних впливів може бути направлена як назовні – на інших людей, громадські структури або на суспільство в цілому, на природне середовище, архітектурні пам'ятники, історичну пам'ять, різні предмети, так і звернена на самого себе – руйнування особистості, здоров'я, суїцид [16].

Конструктивні та деструктивні впливи ІС визначаються рядом властивостей і характеристик, що власне і відображають закономірності його розвитку і функціонування.

Першою важливою особливістю, на яку потрібно звернути увагу, є те, що ІС притаманне постійне і стрімке розширення. Особливо бурхливо розширення інформаційного середовища суспільства відбувається останнім часом, і темпи його постійно зростають. За таких умов людині буває дуже складно розібратися в якості й істиності отримуваної інформації, що створює дезорієнтацію не тільки в інформаційному полі, але й у реальності.

Постійне оновлення ІС призводить до того, що люди навіть не встигають виробляти власну думку з приводу подій, що відбуваються, тому швидше приймають вже готову інтерпретацію запропонованої постачальником інформації, і це негативно позначається на їх здатності до аналітичного, критичного мис-

лення, і, як наслідок, у них знижується імунітет до маніпулятивного впливу. Крім цього, звернемо увагу ще на один важливий момент. У дослідженнях [17] констатується, що великі обсяги інформації змінюють як саму людину, так і сутність суспільних відносин. ІС, що стрімко змінюється, несе новий лад життя, нові правила поведінки, нові уявлення про світ. На арену виводиться Homo Informaticus – «людина інформаційна», у якій занадто мало специфічно людського: звужується сфера безпосередніх, особистих контактів; з'являються нові культурні практики, невідомі раніше; нові правила поведінки, засновані на прагненні до самоізоляції від перманентно вибухонебезпечного світу та ін.

Наступною важливою рисою ІС є складність і неоднозначність. У глобальному масштабі формується принципово нове максимально насичене інформацією складне високоавтоматизоване середовище, що ставить людину в залежність від нього. У такому середовищі для отримання корисної інформації людина змушена обробляти значну кількість різноманітної інформації (найчастіше непотрібної), щоб отримати необхідні відомості. Крім того, людина змушена виробляти механізми захисту від інформаційних впливів із метою забезпечення інформаційно-психологічної безпеки, оскільки поряд з інформацією, яка адекватно відображає факти, в ІС циркулює й деформована, перекручена інформація, часто створена спеціально для введення в оману при досягненні певних цілей. Як підкреслюється в [18], найбільш небезпечним джерелом загроз є істотне розширення можливості маніпулювання свідомістю людини за рахунок формування навколо неї індивідуального «віртуального інформаційного простору», а також можливості використання технологій впливу на її психічну діяльність.

І нарешті, основною характеристикою ІС є «турбулентність» – невпорядкований рух, якому характерна швидка зміна темпів процесів, що відбуваються. Турбулентність ІС означає, що зміни в ньому відбуваються з високим ступенем невизначеності й непередбачуваності. У такому стані не можна однознач-

но визначити характер впливу ІС – чи є сприйнята інформація корисною, нейтральною або шкідливою. Зони турбулентності характеризують вкрай нестійке положення, яке під час найменшого негативного впливу може втратити рівновагу й змінити свій стан. Якщо не вживати належних заходів протидії, виникає хаос.

Вплив інформаційної турбулентності слід розглядати в трьох площинах: державній, суспільній та особистісній.

Якщо розглядати площину держави, то причинами турбулентності можуть бути як внутрішні процеси, зумовлені протиріччями становлення й розвитку в нових умовах світового порядку, так і зовнішніми – цілеспрямованими інформаційними впливами недружніх країн із метою дестабілізувати суспільно-політичну ситуацію, викликати нестабільність і хаос. Відомий німецько-американський психолог Курт Левін підкреслював роль навмисно створюваної турбулентності при веденні психологічної війни: «Один із головних методів придушення морального духу за допомогою стратегії залякування полягає в точному дотриманні такої тактики – тримати людину в стані невизначеності щодо її поточного положення і того, що може чекати на неї в майбутньому. Крім того, якщо часті коливання між суворими дисциплінарними заходами й обіцянкою гарного звернення укупі з поширенням суперечливих новин роблять когнітивну структуру ситуації неясною, то людина втрачає впевненість у тому, призведе її якийсь конкретний план до бажаної мети або ж, навпаки, віддалить від неї. За таких умов навіть ті особистості, які мають чіткі цілі й готові піти на ризик, виявляються паралізованими сильним внутрішнім конфліктом щодо того, що слід робити» (цитується по [19]).

Завдання держави – забезпечити національну безпеку, що має на увазі не тільки її обороноздатність, але й соціальні, економічні, культурні, інформаційні аспекти.

Причому, як підкреслює Щекотин Є.В. [20], необхідний перегляд стратегічного дискурсу в бік відмови від формулюван-

ня безпеки в термінах загроз і переорієнтація на мислення, що спрямоване на управління ризиками національної безпеки. На відміну від загроз ризики підкреслюють динамічний характер викликів, що виникають.

Не можна не погодитися з [21], де стверджується, що першочергова стратегія інформаційної безпеки України полягає в подоланні турбулентності й досягненні керованості. Необхідна систематизація та алгоритмічне використання механізмів для забезпечення внутрішньої інформаційної безпеки і формування підтримки України в суспільствах країн-партнерів.

Доктрина інформаційної безпеки України (затверджена Указом Президента України від 25 лютого 2017 року № 47/2017 [22]) зазначає, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту й розвитку інформаційного простору в умовах глобалізації і вільного обігу інформації. Доктрина розділяє національні інтереси України в інформаційній сфері на життєво важливі інтереси особистості, де в третьому пункті йдеться про захищеність від руйнівних інформаційно-психологічних впливів; і життєво важливі інтереси суспільства й держави, де серед багатьох пунктів значущими в контексті даного дослідження є наступні: усебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірної та об'єктивної інформації; збереження й примноження духовних, культурних і моральних цінностей народу України; розвиток медіакультури суспільства й соціально відповідального медіасередовища; формування ефективної правової системи захисту особистості, суспільства й держави від деструктивних пропагандистських впливів; створення на базі норм міжнародного права системи й механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, насамперед пропаганди; розвиток інформаційного суспільства, зокрема його технологічної інфраструктури.

Із приводу впливу інформаційної турбулентності на суспільство існують різні, іноді діаметрально протилежні погляди. Так, у роботі [23] з оптимізмом стверджується, що «в процесах розвитку турбулентних систем соціальної природи потенція, що відображається спочатку в енергії хаотичних коливань, або інакше, пасіонарності, трансформується з часом на корисну роботу суспільства…». В іншому ж дослідженні, навпаки: «Якщо потрясіння відбуваються занадто часто і їх інтенсивність із кожним разом зростає, є небезпека, що все суспільство буде введено в стан масового психозу … люди будуть роз'єднуватися, намагаючись поодинці втікати від шокових реалій, замикатися в собі, знаходити заспокоєння в запереченні дійсності і в популярних розвагах, але при цьому в будь-який момент будуть готові до спалаху люті» [19]. Ще в одній роботі знаходимо: «… відбувається деградація масової культури, оскільки інформаційна турбулентність, хаос не дозволяють вижити ні високим смислам, ні високим почуттям, стандартна логіка й емоції просто «не доганяють», вони занадто повільні, залишається рефлекс, інстинкт і зоопсихологія афекту. Таким людям не треба нічого пояснювати, ними легко управляти на несвідомому рівні методами НЛП і двадцять п'ятого кадру в період споживання чергової порції інформаційної жуйки» [24].

Беручи до уваги ще одну думку, що «епоха турбулентності, яка почалася, буде дуже важкою для людства; разом із тим вона принесе з собою не тільки негативні й руйнівні, але й позитивні, необхідні для подальшого розвитку наслідки» [25]. Слід зауважити, про це вже було сказано раніше, що на світовий суспільний розвиток значно впливає стан ІС, з яким сучасне суспільство нероздільно пов'язане. Інформаційна турбулентність може в корені поміняти стан речей.

У джерелі [19] підкреслюється найважливіший результат багаторічних досліджень учених в області психології, соціології та психіатрії: щодо кількості змін, які здатна витримати людська свідомість, існують чіткі межі, і в майбутньому події можуть від-

буватися так швидко, що людський мозок не зможе осмислювати інформацію.

При дослідженні шляхів подолання турбулентності крізь призму властивостей особистості, сформовано поняття *«інформаційно-психологічна турбулентність» – нестабільний стан психіки людини, викликаний інформаційним впливом, що виявляється в раптових припливах гніву, печалі або відчаю, відчутті тривоги, роздратування, страху чи смутку.* У такому стані особистість неадекватно оцінює навколишнє оточення й робить нелогічні вчинки.

Безсумнівно, інформаційно-психологічна турбулентність є фактором загроз інформаційно-психологічної безпеки особистості і потрібні заходи з деактивації цього фактору. Стратегічно важливим як для держави, так і суспільства (що і зазначено у вищезгаданій Доктрині) є формування такої політики, де інформаційна культура займає провідне місце. Мається на увазі не тільки накопичення суми знань, а й розвиток фундаментальних навичок мислення і творчості, духовного розвитку особистості. Відповіддю на турбулентні інформаційні виклики може стати розвиток «турбулентного мислення», заснованого на неформальному, евристичному підході до аналізу ситуації і прийняття рішень (досвід, інтуїція, спритність, винахідливість і т.ін.).

Із наведеного слід зробити висновок, що інформаційна турбулентність, яка є наслідком синергетики властивостей інформаційного середовища, є деструктивним фактором інформаційно-психологічної безпеки як по відношенню до держави й суспільства, так і окремої особистості.

Введене нами поняття «інформаційно-психологічна турбулентність», що характеризує нестабільний психічний стан людини, потребує розвитку й подальшого смислового наповнення задля актуалізації державного та суспільного реагування на проблему для вироблення дієвої політики для її вирішення.

2.3. Державні управлінські підходи до забезпечення інформаційної безпеки в умовах турбулентного стану сучасного суспільства

У ході викладення матеріалу в попередніх підрозділах показано, що хаотичні нелінійні процеси в суспільстві, у тому числі й інформаційного характеру, мають вирішальний вплив на життя сучасної людини. Особливого значення в турбулентному суспільстві набуває управління інформаційною безпекою, адже деструктивні явища в цьому аспекті можуть призвести до економічних, соціально-політичних і техногенних зрушень, аж до підриву належного функціонування держави. Тому важливо визначити головні державні управлінські підходи до забезпечення інформаційної безпеки з точки зору констатації турбулентного стану сучасного суспільства.

Вихідним поняттям у даному контексті постає безпека, яка є об'єктом управління. У теорії безпеки життєдіяльності добре відома аксіома про потенційну небезпеку: «Усі дії людини і всі компоненти середовища існування, насамперед, технічні засоби й технології, крім позитивних властивостей і результатів, мають здатність генерувати травмуючі й шкідливі фактори. При цьому будь-яка нова позитивна дія або результат неминуче супроводжуються виникненням нових негативних факторів» [26]. В умовах турбулентного суспільства цей принцип правомірно використовувати для оцінки не тільки технічних, а й соціальних, економічних, політичних систем. Невизначеність середовища, у якому протікає життя людини, нестійкість соціальних і природних процесів змушує розглядати це середовище як потенційне джерело різних небезпек, загроз, факторів ризику й застосовувати запобіжні заходи забезпечення безпеки. Оскільки сучасна людина, окрім природного й соціального, знаходиться ще і в інформаційному середовищі, логічно в цьому контексті вести мову і про інформаційну безпеку.

Сутність управлінських підходів розглядається нами на основі трактування безпеки в термінах управління ризиками. На відміну від загроз ризики підкреслюють динамічний характер викликів, що виникають у турбулентному суспільстві. Найбільш відповідне трактування безпеки в такому ракурсі дає Н. Луман, який ототожнює безпеку зі збереженням і розуміє як відсутність втрат, забезпечену індивідуальною калькуляцією ризиків, успішне конструювання ситуації [27]. Схоже трактування пропонує А.І. Поздняков [28], де безпека визначається як захищеність цінностей суб'єкта (держави, суспільства, особистості) від небайдужого для цього суб'єкта збитку. При цьому можна використовувати простий і зрозумілий критерій рівня небезпеки – ймовірний збиток або ризик у широкому його трактуванні.

Ризик – поняття, що має багато значень, але в даному випадку зрозуміло, що мова йде про можливі події, явища й процеси, наслідки яких можуть мати несприятливий вплив на різні аспекти стану людського життя (у тому числі й на інформаційну безпеку).

Управління безпекою передбачає не тільки розрахунок-вимір ризиків, але також зниження й управління ними. Рівень того чи іншого ризику кількісно характеризує ефективність прийнятих заходів безпеки. Діяльність із їх планування та здійснення є безпосередньою функцією державного управління. Тому доцільно трактувати рівень захищеності населення від впливу інформаційних ризиків, рівень забезпечення інформаційної безпеки як критерій оцінки ефективності управління.

У загальному вигляді інформаційна безпека – *це стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу [29].* У даному визначенні суб'єктами інформаційних відносин можуть бути держава, суспільство, організація, людина.

У контексті національної безпеки інформаційна безпека може розглядатися, з одного боку, як самостійний її елемент,

а з іншого – як інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.ін. У такому руслі більш повним визначенням інформаційної безпеки можна вважати наступне: «інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства й держави, при якому зводиться до мінімуму завдання шкоди через неповноту, невчасність та невірогідність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації» [30]. Але й це визначення не розкриває всю сутність поняття, адже воно дається в статичних категоріях. Найбільш доречним нам видається динамічний підхід, який показує дії задля забезпечення належного стану суб'єкта. Релевантним у цьому плані виглядає визначення А.Д. Урсул, Т.(Ф).Н. Цирдя [31], яке з певними авторськими доповненнями й змінами виглядає наступним чином: інформаційна безпека – «здатність держави, суспільства, соціальної групи, особистості, по-перше, забезпечити з певною ймовірністю достатні й захищені соціальний інтелект і інформаційний ресурс, оптимальну соціальну ентропію й інформаційне середовище для підтримки життєдіяльності та життєздатності, стійкого функціонування й розвитку соціуму; по-друге, протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на індивідуальну та суспільну свідомість і психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації; по-третє, виробляти особистісні та групові навички та вміння безпечної поведінки; по-четверте, підтримувати постійну готовність до адекватних заходів в інформаційному протиборстві, ким би воно не було нав'язане; по-п'яте, постійно й послідовно за певною безпечною програмою «вмонтовувати» штучний інтелект в суспільне середовище».

Щодо сутності державного управління, то воно розглядається в монографії як один із видів соціального в широкому трактуванні, тобто є особливою функцією, що виникає з потреб

суспільства як самодостатньої системи та здійснюється у відповідних державних чи недержавних формах шляхом організаторської діяльності спеціально створеної для цього групи органів. Головне, що система державного управління повинна бути близькою до потреб суспільства, підконтрольною йому, прозорою та ефективною.

Беручи до уваги дослідження Щекотина Є.В. [12,13] та базуючись на власному аналізі, було виділено чотири парадигми управління інформаційною безпекою.

Перша спирається на системний підхід і бере до уваги ряд базових постулатів: система є цілісним і якісно своєрідним утворенням; вона знаходиться в стані динамічної рівноваги із середовищем і здатна самовідтворюватися. Ризик у парадигмі системного підходу потрібно розуміти як порушення рівноваги системи, що виникає внаслідок неузгодженості елементів усередині системи або впливу зовнішніх факторів. В основі управління ризиком лежить максимально повний облік усіх можливих дестабілізаційних факторів, вразливостей як усередині, так і назовні системи.

Управління ризиком повинно бути зосереджене на розробці і впровадженні заходів, що сприяють підвищенню стійкості системи до внутрішніх та зовнішніх чинників нестабільності. Як правило, така сукупність заходів спрямована на посилення контролю над елементами системи, над каналами взаємодії із зовнішнім середовищем. Системний підхід в управлінні ризиками полягає в посиленні заходів контролю, секретності, чіткому розрізненні потенційних загроз і ризиків, калькуляції можливих втрат і т.ін. Такий підхід характерний для систем, де інформаційна безпека є складовою державної, військової, банківської і т.ін.

Друга базується на синергетичному підході, що є розвитком системного підходу. У даному підході розглядаються нелінійні динамічні системи, еволюція яких визначається внутрішніми процесами самоорганізації. Синергетичний підхід в

управлінні спрямований на створення умов для саморозвитку системи, можливостей еволюціонувати в напрямку властивих системі характеристик і цілей.

У синергетичній парадигмі ризик розглядається як ймовірність реалізації катастрофічного сценарію еволюції системи. Система в неврівноваженому стані знаходиться під загрозою руйнування, і в цьому випадку управління ризиком вимагає більше не калькуляції втрат, а здатності передбачати можливі сценарії і проводити попереджувальні дії на ранніх етапах. Враховувати потрібно не тільки системні чинники небезпеки й загрози, а й їх можливе взаємне накладання, резонанс взаємно підсилюючих нелінійних коливань.

У даній парадигмі управління ризиками слід розцінювати як вплив на поведінку системи для того, щоб уникнути руйнівних наслідків. Важливо підкреслити зв'язок ризику й темпоральності явища. У період нестійкості системи ризик різко зростає, чутливість до випадкових факторів загострюється. У зв'язку з цим особливого значення набуває здатність управлінця передбачати траєкторії руху системи за слабкими сигналами.

Прикладом застосування синергетичного підходу в управлінні є сценарні прогнози, наприклад, щодо інформаційного ажіотажу навколо проблеми коронавірусу.

Третя парадигма управління – феноменологічна. Для пояснення її сутності наведемо декілька супутніх понять. Згідно з класичним визначенням Е.Гуссерля, *феноменологія* – дескриптивна наука про сутності трансцендентально чистих переживань у межах безпосередньої інтуїції. *Феноменологічний підхід* – розгляд проблем управління з позицій життєвого досвіду й особистісного сенсу учасників спільної діяльності, тих інтерсуб'єктивних значень предметів, якими люди керуються при прийнятті рішень [32]. *Інтерсуб'єктивність* – здатність людини в процесі комунікації встановлювати співвідношення між декількома точками зору – власної та чужої, тобто враховувати, порів-

нювати, протиставляти, примиряти різні точки зору на об'єкти й події [33].

Виходячи з наведених визначень, можна констатувати, що першочерговими у феноменологічному підході є питання цінностей, значень, переконань людей, дотримання прийнятого порядку і т.ін. Управлінський вплив, щоб бути ефективним, направляється на релевантні предмети життєвого середовища та проблемні життєві ситуації, він повинен враховувати ситуативний характер взаємодії. Умовою ефективного управління є розуміння тієї реальності, у якій живуть різні люди й спільноти, знання механізмів конструювання інтерсуб'єктивності реальності, здатність до виявлення неявних ознак, фонових очікувань, фонових знань, що лежать в основі інтерпретації дій і подій. У цьому контексті доречно згадати введене поняття *турбулентне мис*лення – мислення, засноване на неформальному, евристичному підході до аналізу ситуації й прийняття рішень (досвід, інтуїція, винахідливість і т.ін.), що призводить до формування умов для забезпечення інформаційної безпеки.

У феноменологічній парадигмі ризик пов'язаний із неправильним розумінням, неузгодженістю смислів, якими люди наділяють події й дії, розбіжність ціннісних орієнтирів. Державне управління ризиком має бути спрямоване на прояснення значень, установлення прозорості смислових систем, коригування ціннісних установок суб'єктів взаємодії. Тому величезного значення набуває комунікація, узгодження ціннісно-смислових орієнтирів керманичів і керованих.

Феноменологічний підхід в управлінні інформаційною безпекою важливий, коли мова заходить про оцінку тих чи інших подій і явищ як ризикованих, ступеня їх небезпеки для суспільства, сприйнятті соціальних ризиків і т.ін.

Четвертий підхід – когнітивний, що набув широкого поширення у зв'язку з розвитком концептуальних моделей «суспільства знання», «інформаційного суспільства», «постіндустріального суспільства» і т.п. У всіх цих концепціях підкреслюється

зростання ролі знань і наукомістких технологій для процесу виробництва й управління.

Якщо розглядати ризик із позиції когнітивного підходу, то його можна інтерпретувати як форму знання. Ризик – це знання, інформація про можливі небезпеки. Управління ризиками в рамках даної парадигми пов'язане з кваліфікованою експертизою ситуації, ризик-комунікацією (своєчасним інформуванням суспільства про ризики) і т.ін. Яскравий приклад реалізації когнітивного підходу в управлінні безпекою – це феномен інформаційних війн, який набуває все більшого значення у зв'язку з поширенням засобів масової комунікації.

Повертаючись до визначення інформаційної безпеки, поданим А.Д. Урсул, Т.(Ф.)Н. Цирдя, можемо стверджувати, що кожен із його пунктів тією чи іншою мірою може бути забезпечений наведеними управлінськими підходами. У той же час слід зазначити, що наведені підходи до державного управління, по-перше, не є універсальними й відокремленими в якомусь конкретному випадку, тобто вони мають системний характер, і управлінець повинен уміти комплексно застосовувати підходи залежно від ситуації; по-друге, повинні враховуватися особливості процесу управління, що неминуче виникають у ситуації зростаючої турбулентності в суспільстві, природі та техносфері. Треба брати до уваги той факт, що при аналізі підходів до управління інформаційною безпекою зазвичай береться за основу базове припущення про можливу редукцію ризиків до гомогенної абстрактної схеми їхньої взаємодії. У той же час в умовах соціальної турбулентності особливо важливим виявляється враховувати їх гетерогенність. Так, у випадку системного підходу за основу береться припущення типізації керованих елементів, тобто гомогенність у даному контексті означає встановлення фактичної їх рівності (або, щонайменше, еквівалентності). Абстрактний підхід розширює можливості контролю за поведінкою, обчислення суворих алгоритмів поведінки. Однак у ситуації турбулентності, коли керовані елементи стають «текучими

об'єктами», такі системи стають занадто громіздкими й неефективними. Вони просто не встигають слідом за потоками. Наприклад, Х. Молотч у роботі з характерною назвою «Проти безпеки» показує основні недоліки сформованої «мілітаристської» ідеології [34]. Побудовані за стандартизованими схемами, ці системи безпеки спрямовані на уніфікацію, посилення контролю й неухильне підпорядкування цим абстрактним правилам. На численних прикладах Х. Молотч показує, що такі «мілітаристські» системи виявляються нездатними запобігти терактам і часто самі стають причиною численних неприємностей і навіть небезпеки для населення. Із цього можна зробити висновок, що складні закриті системи, що базуються на посиленні контролю як головному інструменті в забезпеченні інформаційної безпеки методами уніфікації і конструюванні абстрактних типів, закритості й суворому розмежуванні, універсальності правил і схем і т.ін., ефективні для стабільних суспільств, у яких ступінь дифузії, рухливості й проникнення кордонів невелика.

В умовах же соціальної турбулентності потрібні нові підходи, одним із яких може стати концепт гетерогенності. У цьому випадку акцент в управлінні інформаційною безпекою повинен бути зроблений на мікрорівні, тобто на безпосередніх практиках взаємодії, які враховують локальну специфіку й особливості. Держава має зменшити монополію на управління інформаційною безпекою (на цьому вже був зроблений акцент у першому підрозділі) та делегувати більш широкі повноваження місцевому самоуправлінню, суспільним та громадським інститутам, які є більш динамічними в розрахунку-вимірі ризиків і управлінні ними.

Отже, державне управління інформаційною безпекою, що базується на трактуванні безпеки в термінах управління ризиками, враховує динамічний характер викликів, що виникають у турбулентному суспільстві. Слід зазначити, що розглянуті парадигми державного управління, по-перше, не є розмежованими та універсальними, по-друге, повинні враховувати особливос-

ті процесу управління, що неминуче виникають у ситуації зростаючої турбулентності в суспільстві, природі та техносфері. В умовах турбулентності ефективним може стати концепт гетерогенності, де акцент в управлінні інформаційною безпекою переноситься на мікрорівень, тобто на безпосередні практики взаємодії, які враховують локальну специфіку й особливості.

2.4. Стратегічні напрямки державної політики в умовах актуалізації інформаційних викликів епохи турбулентності

Як уже було зазначено, термін «турбулентність» у перекладі з латинської означає «бурхливий, хаотичний, невпорядкований» і використовується при розгляді нелінійних процесів, непередбачуваності подій, різких змін тенденцій, зростанні конфліктності.

У визначенні епохи турбулентності (див. попередній розділ) одним із негативних явищ нами виділено *порушення соціального порядку*. Згідно з класичним визначенням, *соціальний порядок – система, що включає індивідів, взаємозв'язки між ними, урегульовані соціальними нормами (право, мораль, релігія тощо), що сприяють поведінці людей, необхідній для успішного функціонування цієї системи.* Для подальшого розгляду додамо ще одне визначення [35]: *соціальний порядок – стан відносної стабільності, урівноваженості, збалансованості соціальних відносин, діяльності, норм у суспільстві, який задає індивідам, групам, інституціям відповідні моделі поведінки. Соціальний порядок є статичною, емерджентною характеристикою соціальної системи, що інтегрує в собі її цілісність, організованість, гармонійність, унормованість, або структурну, інституціональну, організаційну, функціональну, нормативну впорядкованість.* У соціальному порядку, незважаючи на системність, залежно від площини розгляду можна виділити його форми:

структурний, інституціональний, організаційний, функціональний, нормативний та ін.

Візьмемо до розгляду функціональний порядок, що фігурує як основний (дивись перше визначення) у суспільних відносинах, що перебуває в найбільш динамічному стані, і саме тому він більш за все віддзеркалює риси епохи турбулентності. Відомий соціолог-функціоналіст Артур Стінчкомб [36] за допомогою математичного апарату запропонував оригінальну концепцію пояснення соціальних явищ, де функціональний порядок визначається динамічною взаємодією декількох змінних. Використовуючи його методологію, можна відобразити універсальну модель підтримки рівноваги стану динамічної системи, у тому числі соціального типу (рис. 2.1.).

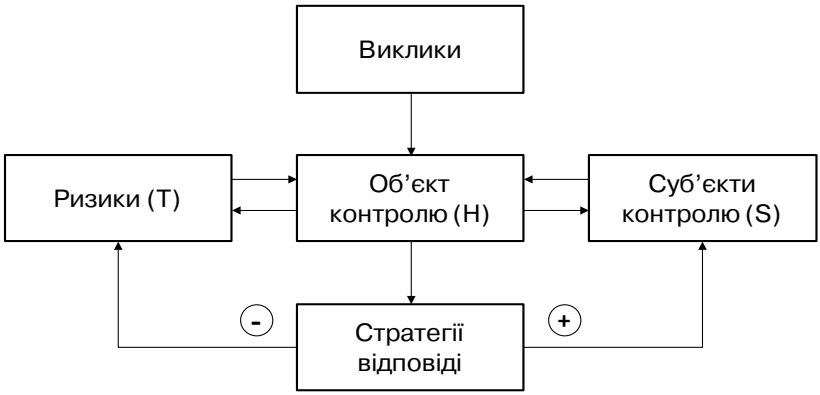


Рис. 2.1. Модель підтримки рівноваги стану динамічної системи

В основі функціональної схеми А. Стінчкомба лежать три елементи: 1) основна, гомеостатична змінна **Н**, яка знаходиться в рівновазі (на рис.2.1. – *об'єкт контролю*) і яка власне відобра-

жає явище; 2) структура підтримки **S** (*суб'єкти контролю*), яка допомагає зберігати стабільність **H** і пов'язана з нею прямим і зворотним зв'язком; 3) напруга **T** (*ризики*) – те, що прагне порушити рівновагу і негативно впливає на **H**. Суть роботи класичної схеми дуже проста. Розглядаються впливи на змінну **H**. Якщо структура підтримки **S1** справляється із завданням стабілізації **H** на заданому рівні, виникає нова **S2**, яка залежно від наявних ресурсів і нових умов буде по-іншому впливати на **H** і яка, у свою чергу, може бути пов'язана з іншими **H**.

У розглянутій моделі (рис.2.1.) було зроблено деякі правки і доповнення. По-перше, у класичній схемі від **H** до **T** немає зворотного зв'язку, тільки «негативна» стрілка від **T** до **H**. Погоджуючись із думкою Н.В. Головко [15], якщо зв'язати **H** і **T** зворотним зв'язком, можна отримати додаткові важелі в поясненні деяких суспільних тенденцій. Чим сильніше тисне **T**, тим менше значення **H**, тим більше зусилля докладає **S** для того, щоб відновити значення **H**. **S** і **T** формально отримують однаковий статус взаємно протидіючих «сил», пов'язаних прямим і зворотним зв'язком з **H**. У певному сенсі тут можна говорити про рівнозначність **T** і **S**, – важливо не те, що структура підтримки знімає негативний ефект напруги, а те, що відновлення значення гомеостатичної змінної одночасно створює умови для порушення її балансу.

По-друге, вводимо елементи «виклики» і «стратегії». Це дає змогу зробити модель більш універсальною, адже ризики для об'єкта турботи виникають тільки за наявності викликів. А стратегії – це реагування на виклики. Вони можуть бути успішними і вести до зменшення ризиків за рахунок покращення контролю суб'єктів, а можуть бути й негативними – тоді підсилюються ризики.

Запропонована модель пояснює причини порушення стабільності будь-якої системи, оскільки вказує на різні варіанти можливої конфігурації:

– поява нових незвичних викликів і ризиків (зовнішніх і внутрішніх);

– провал колишніх суб'єктів контролю (інститутів, організацій, практик), надмірні витрати й незаплановані негативні наслідки їхньої діяльності;

– неадекватні стратегії відповіді на виклики;

– нерелевантність об'єктів контролю, виражених через цінності, принципи і правила умовам, що змінилися.

До явищ, що зазвичай включаються у зміст нинішньої кризи глобальної стабільності, можна віднести:

1) затяжні військові конфлікти, формування зон насилля й соціальних лих, багаторічні зусилля з подолання яких досі не мають результату (арабо-ізраїльський конфлікт, Сирія, Лівія, Донбас та ін.);

2) зростання напруженості між країнами-лідерами, конфлікти всередині Євросоюзу;

3) тероризм, загрози з боку міжнародних кримінальних спільнот і мереж;

4) міграційна криза в Європі, майже повсюдне зростання ксенофобії, зрушення в напрямку політики закритих дверей та протекціонізму;

5) істотне зниження авторитету, ролі, впливу ООН, ЮНЕСКО та інших міжнародних організацій;

6) глобалізація економічних криз, посилення соціальних протестів, революційні хвилі;

7) розчарування в демократії, зліт популярності авторитарних лідерів, установлення популістських режимів;

8) почастішання природних катаклізмів, для подолання яких часто не вистачає ресурсів;

9) негативні тенденції, що пов'язані з новітніми інформаційними викликами.

Уважний розгляд наведених явищ показує, що кожне з них може бути віднесене до якогось елементу запропонованої мо-

делі (див. рис. 2.1.). Наприклад, вищезазначений п.5 указує на послаблення суб'єктів контролю.

Повноцінний аналіз причин масштабних і різнорідних явищ турбулентності у відповідності до цієї схеми сумірний не статті, а серії багатьох дослідницьких проєктів. Зазначимо, що темою нашого дослідження є тільки розгляд 9-го пункту в наведеному списку. Але і це також великий обсяг досліджень, тому будуть розглянуті тільки фактори, які представляються найважливішими.

Використовуючи модель, можливо не тільки пояснити причини порушення рівноваги стану динамічної системи, а й дослідити процес вибору стратегій щодо її збалансування. Так, вона буде застосовуватися під час аналізу інформаційних викликів.

Насамперед необхідно зазначити, що сформований у сучасній соціології погляд на турбулентність можна охарактеризувати як «стурбованість» – турбулентність оцінюється як деякий системний виклик, як тимчасовий стан транскордонного переходу до більш стабільного стану. Однак доцільно зазначити, що такий погляд не є очевидним. Можливо, що сьогоднішні нестабільність і нестійкість – це якраз риси найближчого майбутнього, у якому нам доведеться жити. Констатація турбулентності сучасного суспільства ставить ряд серйозних завдань перед управлінням (суб'єктами контролю згідно з рис. 2.1.). Щодо останнього, у контексті даного дослідження потрібно надати деякі пояснення. Насамперед, управління – поняття складне й багатогранне, воно залежить від специфіки об'єкта. За визначенням Соловйова В.М., у загальному розумінні управління – це цілеспрямований вплив на складну систему [37]. У більш конкретному розумінні, управління, з точки зору Пилипишина В.П. [38], являє собою діяльність уповноважених органів, що спрямована на досягнення конкретних завдань за допомогою управлінських методів, способів та функцій.

Розглядаючи управління крізь призму держави, звернімо увагу на особливості його трактування: управління держави, коли остання виступає суб'єктом діяльності щодо виконання законів та інших правових актів органів державної влади; і державне управління, яке розглядається як один із видів соціального в дотриманні суспільного порядку і є особливою функцією, що виникає із потреб суспільства як самодостатньої системи та здійснюється у відповідних державних чи недержавних формах шляхом організаторської діяльності, спеціально створеної для цього групи органів. Таке управління має також політичний характер і може розглядатися з соціальної, економічної точок зору. Саме в цій інтерпретації ми розглядаємо державне управління в нашій моделі. Головне, що пріоритетами діяльності демократичної держави повинно бути забезпечення реалізації прав, свобод і законних інтересів її населення, служіння йому. У зв'язку з цим система державного управління має бути близькою до потреб і запитів простих людей, підконтрольною суспільству, прозорою та ефективною.

При подальшому розгляді моделі очевидним є те, що об'єктом контролю є інформаційна безпека, а ризики – усе те, що її порушує, включаючи такі поняття, як небезпека, загроза, уразливість. Між цими концептами, безумовно, існує відмінність, проте в рамках даної роботи не постає завдання детального розгляду дефініцій цих понять.

Сформувавши всі компоненти моделі в загальному вигляді, розкриємо сутність її роботи при конкретизації інформаційних викликів. До розгляду взято 2 варіанти: 1) турбулентні інформаційні виклики держави; 2) турбулентні інформаційні виклики особистості. Виходячи з логічного міркування, у першому випадку об'єктом буде інформаційна безпека держави; у другому – інформаційно-психологічна безпека особистості.

Вище зазначено, що поняття «інформаційна безпека» може трактуватися як в статичних, так і в динамічних категоріях. Статичний підхід характеризує власне стан об'єкту. Напри-

клад, із точки зору державницького підходу, під інформаційною безпекою розуміється стан захищеності національних інтересів в інформаційній сфері при збалансованості потреб особистості, суспільства і держави. Більш загальне визначення дає Р.М. Юсупов. Він стверджує, що «… інформаційна безпека відповідного суб'єкта (особистості, суспільства, держави, будь-якої системи) може бути визначена як стан, у якому йому (суб'єкту) не може бути завдано істотної шкоди шляхом впливу на його інформаційну сферу» [39].

Динамічний підхід показує дії задля забезпечення належного стану суб'єкта. Показовим у цьому випадку є визначення, дане М.В. Арсентьєвим: «інформаційна безпека – це зняття інформаційної невизначеності щодо об'єктивно і суб'єктивно існуючих потенційних і реальних загроз за рахунок контролю над світовим простором і наявності можливостей, умов і засобів для відсічі цих загроз. Усе це в сукупності визначає рівень (ступінь) інформаційної безпеки кожного суб'єкта» [40]. Як можна побачити, визначення в цілому охоплює роботу нашої моделі. Адже тут є й об'єкт (власне інформаційна безпека», і ризики (загрози), і стратегія (контроль над світовим простором), і суб'єкт у якості управління (наявність можливостей, умов і засобів для відсічі загроз), і позитивний результат (зняття інформаційної невизначеності). Заради справедливості, слід зазначити, що наявність фрази «контроль над світовим простором» відносить дію моделі до першого із вибраного для аналізу інформаційних викликів. Але це не заперечує те, що динамічний підхід методологічно більш функціональний і універсальний. Візьмемо до уваги ще одне визначення (А.Д. Урсул, Т.(Ф.)Н. Цирдя [31]), яке вже розглядалося в попередньому підрозділі і яке релевантно співвідноситься до нашого розгляду викликів, показуючи згідно з нашою моделлю ризики і стратегії дій.

Беручи до розгляду інформаційне протиборство (у вигляді інформаційної війни), як турбулентний інформаційний виклик державі, мусимо визначити згідно з удосконаленою моделлю

характерні ризики щодо об'єкту захисту, а також вибрати адекватну стратегію згідно з моделлю, тобто фраза «підтримувати постійну готовність до адекватних заходів», як це звучить у визначенні, повинна бути наповнена смисловим контекстом.

Спираючись на дослідження О.Н. Яницького [6, 41], в аспекті ризиків виділимо наступне:

По-перше, сьогодні інформаційна війна – супутній елемент будь-якої соціально-політичної кризи, тим більше, якщо він переходить у фазу збройного протистояння. Більш того, інформаційна війна є інструментом створення критичних ситуацій, тобто вона, як правило, розпочинається задовго до виникнення реального конфлікту між соціальними групами, державами та їхніми «кластерами».

По-друге, в основі будь-яких малих і великих інформаційних війн лежить відповідна інтересам «нападника» картина світу (система ціннісних постулатів), на основі якої потім інтерпретуються всі наступні події в решті світу. Тому система цінностей у руках «нападника» – його потужна зброя.

По-третє, невід'ємною характеристикою цих війн є маніпулювання свідомістю «противника», яке здійснюється за допомогою двох основних інструментів: перемикання й перепрограмування. При цьому ніякі дискусії щодо конкретного інформаційного приводу не допускаються. Експерти й очевидці з обох боків прагнуть «викрити міфи», створені протилежною стороною. Тому дискурс цих війн завжди директивний (дефінітивний), ствердний, а не діалогічний або рефлексивний.

По-четверте, інформаційні війни, використовуючи парадигму «свій-чужий» («ми-вони», «друзі-вороги»), свідомо спрощують картину відносин усередині сучасного надскладного суспільства. Зворотний бік цієї медалі – мобілізація суспільства або груп протистояння, набуття ними морально-політичної єдності, часто помилкової, але необхідної для досягнення переваги «своїх» над «чужими».

По-п'яте, головним тактичним прийомом інформаційної війни є нанесення «випереджувального удару», виходячи з розрахунку, що будь-які наступні спростування «противника» вже ніколи не будуть прийняті до уваги міжнародною громадською думкою.

По-шосте, «картинка» або інформаційний ряд завжди певним чином емоційно навантажуються. Інформаційна війна – це не зіткнення потоків об'єктивної інформації. Це війна на розвінчання, придушення або переконання протилежного боку, у якій використовуються емоційні кліше, розраховані на легкість їх засвоєння масовою свідомістю ймовірного противника. Недарма в таких «боях» часто вживається лексикон вуличного або кримінального сленгу.

Нарешті потребують уваги також ризики, пов'язані зі специфічною складовою інформаційної війни – кібервійною, де «військові дії» здійснюються не фізичним, а електронним способом, і де в якості зброї виступає інформація, а інструментами є комп'ютери та Інтернет.

У якості стратегії в моделі (див. рис. 2.1.) нами вибране *забезпечення інформаційно-цифрового суверенітету держави*. Із урахуванням робіт інших дослідників (Владимирова Т.В. [42], Ашманов І.С. [43]), розглянемо її сутність.

Елементами традиційного суверенітету є воєнний, економічний, політичний, культурно-ідеологічний компоненти. До них в останні роки приєднався новий – інформаційно-цифровий. В епоху турбулентності відбувається «розмиття» рамок суверенітетів, а відсутність інформаційно-цифрового компонента може призвести до втрати суверенітету держави взагалі. Остання фраза ще раз підкреслює універсальність нашої моделі. Адже суверенітет може розглядатися і як об'єкт контролю.

Беручи до розгляду суверенітет у визначенні «інформаційно-цифровий», ми підкреслюємо його двоїсту структуру, тобто інформаційні та кібер-компоненти.

Вибрана стратегія означає, що держава повинна мати наступні права і можливості:

– самостійно визначати національні інтереси в цифровій сфері;

– самостійно вести внутрішню і зовнішню інформаційну політику;

– володіти власними інформаційними ресурсами й розвивати інформаційну інфраструктуру держави;

– контролювати електронну та інформаційну безпеку держави.

На цій підставі держава, виконуючи свої функції, забезпечує:

1. «Стійкість» до дій кіберагресора: захист від руйнування інфраструктури, вірусів, атак, зломів, витоків, крадіжки даних, спаму; стійкість до електронних атак (моніторинг, виявлення, попередження, блокування, контратаки).

2. «Стійкість» до умов інформаційної війни: самостійне управління інформацією (фільтрація інформаційних потоків, поширення інформації та ін.); стійкість до інформаційних атак (можливості виявлення, попередження, блокування інформації та контратаки).

Інформаційно-цифровий суверенітет держави охоплює два важливі напрямки:

1. Медійна інфраструктура, до складу якої входять пошукові машини, довідкові ресурси; соціальні мережі, месенджери, блоги, форуми, розсилки;

Інтернет-ЗМІ, традиційні ЗМІ і ТБ; відео-хостинги і фотохостинги; тематичні ресурси (рейтинги / аналітика, історія, наука, автомобілі, спорт, кіно, книги); додатки для соціальних мереж і мобільних пристроїв; дитячий Інтернет.

2. Засоби пропаганди та інформаційних війн: аналіз медійного середовища, моніторинг трафіку й соціальних медіа; кошти фільтрації трафіку; законодавство про відповідальність за контент (хостерів, провайдерів доступу та медійних провай-

дерів); кошти поширення контенту: ЗМІ, блоги, соціальні мережі; сили для поширення контенту – спеціальні підрозділи й засоби для інформаційних війн у мережі.

Окремим важливим елементом інформаційно-цифрового суверенітету є сфера ідеологічної роботи. Наскільки суверенітет держави забезпечується ідеями й наскільки вони конкурентоспроможні, ці фактори стають вирішальними в забезпеченні не тільки інформаційної, а і взагалі безпеки держави.

У другому анонсованому варіанті (турбулентні інформаційні виклики особистості) в проекції на окреслену модель основним ризиком визначаємо турбулентність інформаційного середовища, яка породжує явище інформаційно-психологчної турбулентності (нестабільний стан психіки людини, викликаний інформаційним впливом, що виявляється в раптових припливах гніву, печалі або відчаю, відчутті тривоги, роздратування, страху чи смутку).

Побічним супроводжуючим негативним процесом є вплив кіберпростору. За словами І.С. Ашманова, користувачі «стрімко дурнішають». У Твіттері, Фейсбуці немає «пам'яті», контент тоне в швидкості змін різноманіття інформації. Мислення користувача стає кліповим. Зростає жорстокість і поляризація думок, підвищується градус дискусій. В Інтернеті втрачаються цінності та норми: вкидання дезінформації, обман, пропаганда, спам стають звичайними практиками. У соціальних мережах активно оперують професіонали, у тому числі спільноти «спамерів», діють технологічні системи «відмивання» новин та інформаційних вкидань.

Формуючи далі модель, виходячи з попереднього, об'єктом небезпечного інформаційного впливу й інформаційної безпеки можуть виступати свідомість і психіка особистості.

Щодо суб'єктів інформаційної безпеки, то такими слід вважати ті органи і структури, які в тій чи іншій мірі займаються її забезпеченням. Особистість також може виступати суб'єктом, хоча й займає при цьому найбільш вразливу позицію в забез-

печенні своєї інформаційної безпеки. Адже вона є складовою самої біосоціальної системи, що підлягає захисту (людина, її психіка, моральний і духовний світ, соціально-політичні, психологічні орієнтації, установки, відносини, раціональні та ірраціональні аспекти поведінки, системи громадської думки і прийняття рішень). Сучасну ситуацію, різноманіття її небезпек і загроз філософи (наприклад, С.А. Бочан [44]) характеризують як тотальну залежність особистості від інформаційної культури й комп'ютерної реальності, яка призводить до формування технократичного мислення. Оскільки життєве середовище особистості перетворюється на простір віртуальної комунікації, яка має правила, незалежні від національних і традиційних культур, реальна цілісність особистості підміняється віртуальною, формується новий соціальний тип особистості мережевого співтовариства зі своїми моральними, психологічними та соціальними якостями. З'явився вже новий виразний термін – «інформаційна особистість».

Вибираючи стратегії, мусимо визнати, що тут провідна роль належить державі. У подібному руслі міркує, наприклад, і С.А. Бочан, вбачаючи рішення в активності самої особистості. Утрата колишньої ідентичності в сучасній реальності, на її думку, змушує цілісну особистість вибирати, співставляти запропоновані суспільством нові інформаційні цінності та норми, які допомагають виробити необхідну стратегію поведінки в сьогоденні і в майбутньому. «Народжується новий тип особистості, носій інформаційної культури – «багатовимірна людина», для якої характерне визнання рівнозначності всіх її проявів інтелекту, здатність до інновацій, ризику, мобільності в мінливих ситуаціях».

Державна стратегія інформаційної безпеки має передбачати, насамперед, виконання базових принципів її втілення. Одним із найважливіших є принцип балансу інтересів особистості, суспільства й держави. Очевидно, що особистість зацікавлена в конфіденційності інформації про інтимне життя, доходи і т.ін. Але суспільство зацікавлене в інформації про антисоціальні

прояви, корупцію і т.п. Державні органи взагалі хотіли б знати все про громадян. Показовим є факт віртуального супроводу через мобільний телефон громадян під час коронавірусу в ряді країн.

Другий принцип – це принцип законності та правої забезпеченості. Зростання значущості інформаційної безпеки явно випереджає розвиток відповідної сфери права, чим уміло користуються і політики, і засоби масової інформації, і просто шахраї.

Третій – держава по відношенню до особистості має виконувати більш партнерські, а не насильницькі функції.

З урахуванням указаних принципів стратегію державного управління слід розглядати в декількох площинах:

– юридична – забезпечення юридичних прав і підвищення рівня можливостей населення для доступу до інформаційних ресурсів;

– організаційно-правова – контроль та регулювання інформаційних потоків, створення цивілізованого інформаційного простору країни, надання йому таких властивостей, як цілеспрямованість, системність, стійкість, безпечність;

– соціально-політична – цілеспрямоване використання нових технологій для розвитку демократичної відкритої держави, заснованої на принципах діалогу з населенням;

– науково-технологічна – збереження незалежності свободи слова в процесі поширення інформації в будь-якому технологічному середовищі;

– соціально-культурна – захист національної мови, культурних цінностей від експансії в інформаційній сфері, збереження художнього та наукового спадку;

– психологічна – турбота про психологічне здоров'я населення, особливо молодого покоління;

– педагогічна – переорієнтація освітньої системи відповідно до запитів інформаційного суспільства, впровадження нових форм навчання.

Важливість останнього полягає в тому, що за допомогою поширення відповідних знань з'являється можливість впливати на когнітивний компонент інформаційно-психологічної безпеки. Проводячи практичні заняття, тренінгові заходи, можна позитивно впливати на розвиток навичок критичного мислення, психологічні ресурси особистості, тобто підвищувати рівень суб'єктності особистості у формуванні оптимального рівня інформаційно-психологічної безпеки.

Таким чином, запропонована авторська модель підтримки рівноваги стану динамічної системи дозволяє окреслити ризики викликів епохи турбулентності та сформувати стратегічні напрямки державної інформаційної політики. Викладені теоретичні засади визначення ризиків різної етіології та відповідного стратегічного реагування в умовах турбулентності можуть бути основою для подальшого розвитку державної інформаційної політики.

Список використаних джерел

1. Панченко О.А. Психологические аспекты турбулентности информационной среды. Причорноморські психологічні студії. 2017. Вип.1. С. 3–7.

2. Панченко О.А. Турбулентность в информационной безопасности личности. Клінічна інформатика і телемедицина. 2017. Т. 12. Вип. 13. С. 124–129.

3. Панченко О.А. Психологическая турбулентность в условиях информационной войны. 2018. URL: http://www.psyh.kiev.ua/Панченко_О.А._Психологическая_турбулентность_в_условиях_информационной_войны (дата звернення: 21.03.2020).

4. Панченко О.А. Турбулентність мислення в структурі інформаційно-психологічної безпеки особистості. Психологія і особистість. 2019. № 1(15). С. 35–53.

5. Панченко О.А. Информационно-психологическая безопасность в эпоху турбулентности. монография. К.: КВИЦ. 2020. 472 с.

6. Яницкий О.Н. «Турбулентные времена» как проблема общества риска. Общественные науки и современность. 2011. № 6. С. 155-164.

7. Панченко О.А., Пархоменко-Куцевіл О.І., Антонов В.Г. Інформаційні виклики епохи турбулентності в державному управлінні. Публічне управління та митне адміністрування. Вип. 2 (25). 2020. С. 196-204. URL: https://doi.org/10.32836/2310-9653-2020-2.34

8. Яницкий О.Н. Социобиотехнические системы: новый взгляд на взаимодействие человека и природы. Социологическая наука и социальная практика. 2016. № 3. С. 5–22.

9. Клименко С. Теория и практика ведения «гибридных войн» (по взглядам НАТО) 2015. Зарубежное военное обозрение 2015. № 5. С. 109 -112.

10. Vinsent Mosco. Becoming Digital: Toward a Post-Internet Society. London: Emerald Publishing Limited. 2017. 227p.

11. Vanderburg W.H. Our battle for the human spirit : scientific knowing, technical doing, and daily living. Toronto: University of Toronto Press. 2016. 421p.

12. Щекотин Е.В. Социальное управление в турбулентном обществе: вопросы безопасности и риска. Социум и власть. 2016. № 1 (57). С. 87-92.

13. Щекотин Е.В. Проблема благополучия в турбулентном социуме: аспект безопасности. Вестник науки Сибири. 2017. №4 (27). С. 74-83

14. Beck U. The Metamorphosis of the World. Cambridge: Polity Press, 2016. 223 p.

15. Панченко О.А. Турбулентні соціально-психологічні виклики в системі державного управління інформаційною безпекою. Теорія та практика державного управління. 2020. Том 1. № 68. С. 210-217. URL: http://tpdu.journal.kharkiv.ua/index.php/tpdu/article/view/159/142 (дата звернення: 28.01.2020).

16. Шаршов И.А., Макарова Л.Н.. Изменяющаяся внешняя информационная среда: анализ конструктивного и деструктив-

ного потенциала. Социально-экономические явления и процессы. №4(038). 2012. С. 170-176.

17. Цуканов Е.А.: Информационная среда как фактор социального и нравственного здоровья человека: автореферат диссертации. 2003. URL: http://www.dissercat.com/content/informatsionnaya-sreda-kak-faktor-sotsialnogo-i-nravstvennogo-zdorovya-cheloveka#ixzz4ZK2Ubcmb (дата звернення: 28.01.2020).

18. Емельянов Г.В, Стрельцов А.А. Особенности информационного общества. Информационное общество. Вып.2. 1999. С. 15-17.

19. Даниэль Эстулин. Тавистокский институт (перевод П. Смирнов). Минск, 2014. URL:http://coollib.com/b/284081(дата звернення: 28.01.2020).

20. Щекотин Е.В. Национальная безопасность в условиях турбулентности: критический обзор. Международный научный журнал «ИННОВАЦИОННАЯ НАУКА» № 10. 2015. С. 55-56.

21. Александр Смирнов. Коммуникационная стратегия информационной безопасности Украины. URL: http://hvylya.net/analytics/politics/kommunikatsionnaya-strategiya-informatsionnoy-bezopasnosti-ukrainyi.html (дата звернення: 28.01.2020).

22. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення: 28.02.2017).

23. Резеньков Д.Н., Приходько С.С. Понятие «социальная турбулентность» в современном мире в концепции информационной безопасности России. Культура и общество: история и современность. Материалы II Всероссийской (с международным участием) научно-практической конференции. Под редакцией Колосовой О.Ю, Гударенко Р.Ф., Ряснянской Н.А, Красиковой Е.А. Ставрополь. Издательство ООО «Ветеран».2013. С. 128-130.

24. Буданов В.Г. Метаморфозы социальной реальности эпохи перемен: онтологии и технологии. Творческие поиски ученых Израиля и мира сегодня. Сборник статей. Международный центр научных исследований и практики творчества. Израиль – Ашкелон. 2013. С.68-74.

25. Пантин В.И. Первая половина XXI века: «эпоха турбулентности» в мировом развитии. История и современность. № 2. 2008. С. 3-9.

26. Безопасность жизнедеятельности: учеб. для вузов. Под общ. ред. С.В. Белова. М.: Высшая школа. 1999. 40 с.

27. Luhman N. Risk: a sociological theory. N.Y.: Aldine de Gruyter. 1993. 236 p.

28. Поздняков А. И.. Сравнительный анализ основных методологических подходов к построению теории национальной безопасности. Национальные интересы: приоритеты и безопасность. 2013. №21 (210). С. 46-53.

29. Панченко О.А. Банчук Н.В. Информационная безопасность личности: монография. Киев: КИТ. 2011. 672с.

30. Ільницька Уляна. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. URL: http://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf. (дата звернення: 13.05.2020).

31. Урсул А. Д., Цырдя Т. (Ф). Н. Информационная безопасность. Сущность, содержание и принципы ее обеспечения. URL: http://security.ase.md/publ/ru/pubru22.html (дата звернення: 13.05.2020).

32. Социология управления: теоретико-прикладной толковый словарь. Отв. ред. А.В. Тихонов. М.: КРАСАНД. 2015. 480 с.

33. СКоДис. URL: http://scodis.ru/студентам/глоссарий/интерсубъективность/ (дата звернення: 13.05.2020).

34. Molotch H. Against Security: How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger. Princeton, Oxford: Princeton University Press. 2014. 288 p.

35. Соціологія: короткий енциклопедичний словник. URL: https://subject.com.ua/sociology/dict/422.html (дата звернення: 10.04.2020).

36. Stinchcombe A. Constructing Social Theories. Chicago: University of Chicago Press. 1987. 320p.

37. Соловйов В. М. Поняття і сутність правового регулювання державного управління в Україні. Університетські наукові записки. 2007. № 3 (23). С. 27–33.

38. Пилипишин В. П. Поняття та основні риси державного управління. Юридична наука і практика. 2011. № 2 . С.10-14.

39. Юсупов Р. М. Информационное обеспечение национальной безопасности. Национальная безопасность 2010. № 7/8. С. 87.

40. Арсентьев, М. В. К вопросу о понятии об информационной безопасности. Информационное общество. 1997. № 4–6. С. 48–50.

41. Яницкий О.Н. Социология критических состояний общества: теоретические и методические проблемы. Социологическая наука и социальная практика. 2014. №4 (8). С. 5-24.

42. Владимирова Т.В. Обеспечение безопасности в условиях информационной нестабильности общества: диссертация доктора философских наук. Красноярск. 2016. 300 с. URL: http://elib.sfu-kras.ru/handle/2311/26221 (дата звернення: 14.04.2020).

43. Ашманов И. Цифровой суверенитет – новая реальность. 2013. URL: http://eurasian-defence.ru/sites/default/files/doc/ashmanov.pdf (дата звернення: 14.04.2020).

44. Бочан С.А. Проблема целостности личности в информационном обществе: автореф. дис. канд. филос. наук. Ростов-на-Дону. 2007. URL: https://www.dissercat.com/content/problema-tselostnosti-lichnosti-v-informatsionnom-obshchestve/read/pdf (дата звернення: 14.04.2020).

РОЗДІЛ 3

Комунікаційна стратегія як складова державного управління інформаційною безпекою

3.1. Комунікаційні технології – джерело інформаційної безпеки

Кінець 1990-х початок 2000-х рр. стали часом розвитку масової інформатизації, тобто організаційно-забезпеченого процесу задоволення інформаційних потреб індивідів на основі впровадження інформаційно-комунікаційних технологій (далі ІКТ) у всіх областях людської діяльності (державному управлінні, виробничому секторі економіки, освіті, охороні здоров'я) та в приватному житті громадян.

Безсумнівний успіх комп'ютеризації державного управління, судової і правоохоронної систем проявився в підвищенні оперативності та ефективності прийняття державними органами рішень. Виявився вірним і проголошений курс на формування інформаційного суспільства, тобто якісно нового рівня суспільного розвитку на основі високорозвиненої інформаційної інфраструктури, широкого доступу до інформації, збалансованого ринку інформаційних продуктів і підвищення питомої ваги сектора ІКТ в економіці.

Розвиток технологій збору й аналізу даних, обміну ними, управління виробничими процесами здійснюється на основі впровадження когнітивних технологій, їх конвергенції з нано- і біотехнологіями. Значне збільшення обсягу даних, джерелами і засобами поширення яких є промислові та соціальні об'єкти, різні електронні пристрої, призводить до формування нового рівня наукомістких інформаційних технологій. Їх повсюдне застосування сприяє переходу до цифрової економіки.

Інформаційна сфера стала системоутворюючим фактором суспільного життя, тобто цілком обґрунтовано можна

стверджувати, що в життєдіяльності суспільства вона грає не допоміжну роль, а одну з ключових, у тому числі з точки зору державної політики та державного управління. У свою чергу, інформація стає важливим ресурсом суспільства й держави і, як наслідок, суттєво зростає роль засобів масової інформації. Основними каналами передачі інформації є засоби масової комунікації, тобто органи публічної передачі інформації за допомогою технічних засобів, яких на сьогоднішній день стає все більше (рис. 3.1.).

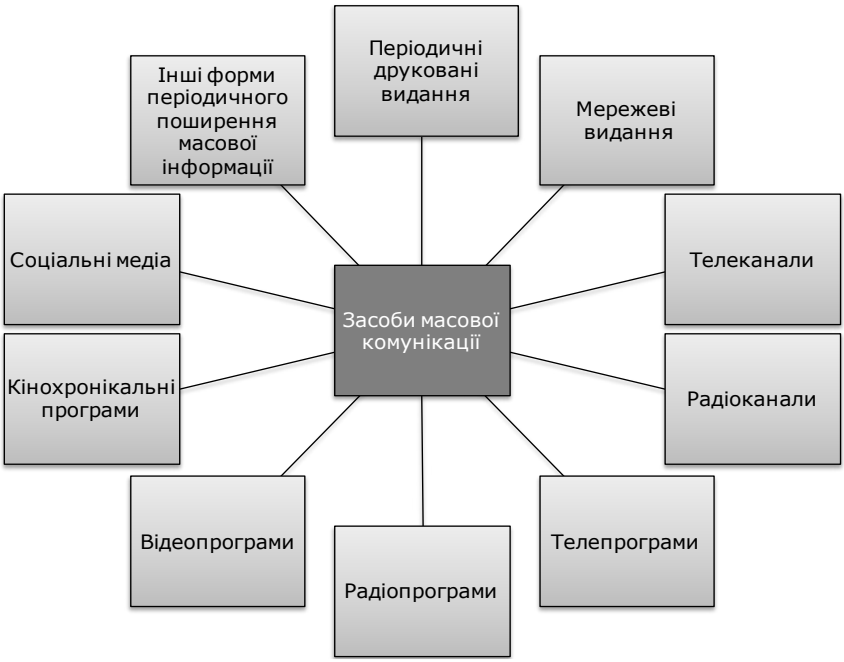


Рис. 3.1. Класифікація засобів масової комунікації

Серед представлених на рисунку загальновідомих каналів передачі інформації слід відзначити радіо, телебачення, періодичні друковані видання, а також визначити ще досить нові та ті,

що набирають усе більшу масу отримувачів інформації, а саме мережеві засоби масової комунікації та глобальної мережі Інтернет.

Проблема дослідження можливостей мережевих засобів масової комунікації особливо актуальна, це обумовлено тим, що в умовах економічного спаду, політичної нестабільності й загострення протиріч між інтересами різних груп населення без розуміння ролі, значення та функцій сучасних засобів комунікації неможливе ефективне управління соціально-політичними процесами. Від розумності і виваженості політики в області розвитку мережевих комунікацій, а також виробництва інформації та її поширення в глобальному інформаційному просторі значною мірою залежить благополуччя країни та її місце у світовій цивілізації.

Виходячи з представленої класифікації, у наступному розділі даної монографії будуть представлені форми подачі інформації та визначено їх вплив на державу, суспільство й особистість. Зараз розглянемо загальну дію і соціальні можливості засобів масової інформації сучасності.

Засоби масової інформації, будучи елементом масової комунікації, формують громадську думку, культуру і світогляд, які істотно впливають на сталий розвиток держави, політичні процеси в суспільстві. Інформаційно-психологічний вплив на людину з боку інформаційної середовища досить суперечливий, тому що поряд із конструктивними властивостями вона володіє й деструктивними. Останні значною мірою визначаються турбулентністю інформаційного середовища, зокрема тими змінами, що відбуваються з високим ступенем невизначеності й непередбачуваності. У такому стані не можна однозначно визначити характер впливу інформаційного середовища: чи є сприйнята інформація корисною, нейтральною або шкідливою. Зони турбулентності характеризують вкрай нестійке положення, яке під вагою найменшого негативного впливу може втра-

тити рівновагу й змінити свій стан. Якщо не вживати належних заходів протидії, виникає хаос.

Серед численних проблем національної безпеки значне місце займає проблема інформаційної безпеки. Невипадково в Загальній декларації прав людини вказується, що реалізація прав людини, у тому числі й на інформацію, є «основою свободи, справедливості та миру в усьому світі».

ЗМІ перетворилися в «четверту» владу, від якої багато в чому залежать зміни, що відбуваються. Саме тому проблема створення систем інформаційної безпеки держави є настільки актуальною на сучасному етапі.

У сучасному світі інноваційних технологій інформаційна безпека вже зараз є соціальним і тільки потім чисто технічним явищем. Її не можна ототожнювати лише із застосуванням спеціальних технічних засобів і методів для захисту інформації від несанкціонованого доступу, викрадення, знищення тощо [1]. Забезпечення інформаційної безпеки – це не тільки захист інформації, але ще й організаційні, правові та інші заходи, спрямовані на забезпечення сталого, стабільного розвитку суспільства й держави, за допомогою яких досягаються цілі захисту національної, економічної безпеки.

Інформаційна безпека проявляє себе не тільки як один із самостійних і самодостатніх видів безпеки, але і як специфічний зріз інших видів безпеки: економічної, соціальної, політичної, військової, духовно-ідеологічної тощо. У такій якості інформаційна безпека виступає синтетичною, інтегруючою підставою для інших видів безпеки, що розкриває й уточнює їх прогресивно-цивілізаційний зміст. З іншого боку, інформатизація суспільного життя є таким засобом соціалізації, наслідком якого виступає певний рівень інформаційної культури – життєво важливої цінності суспільства, держави й особистості як об'єкта національної безпеки [2].

Інформаційна безпека тісно пов'язана з правовим захистом інформаційного простору від руйнівного впливу нега-

тивних факторів. Під міжнародною інформаційною безпекою розуміють такий стан глобального інформаційного простору, при якому виключені можливості порушення прав особистості, суспільства та прав держави в інформаційній сфері, а також деструктивного і протиправного впливу на елементи національної критичної інформаційної інфраструктури [3].

Засоби масової інформації, звернені насамперед до масової аудиторії, природою своєю покликані забезпечити масово-інформаційну безпеку (МІБ) за рахунок «доставки» споживачам необхідних для прийняття рішень інформаційних ресурсів, захисту від маніпулятивної дезінформації, яка поширюється тими ж ЗМІ.

МІБ більшою мірою залежить від такого інформаційного порядку в суспільстві, при якому досягається максимальний рівень інформаційного забезпечення демократії за рахунок всебічної інформованості громадян [4]. Засоби масової комунікації та органи державної влади повинні повідомляти для загального відома інформацію, яка стала їм відома при здійсненні своєї діяльності:

• якщо вона може запобігти загрозі життю або здоров'ю громадян;

• якщо потрібно припинити повідомлення недостовірної інформації;

• якщо вона має або може мати суспільно значимий характер.

Серед проблем інформаційної безпеки держави та її забезпечення однією з найгостріших, найнебезпечніших і важких для вирішення є проблема інформованості населення про діяльність органів законодавчої, виконавчої та судової влади, органів місцевого самоврядування (далі – органи влади). Гострота й небезпека цієї проблеми, життєва необхідність і складність її вирішення обумовлені широкою сукупністю обставин. Ідеться, перш за все, про інформованість як проблему не окремої особистості, спеціальної групи, а всього населення держави.

Населення (багатонаціональний народ), як відомо, є основою і суб'єктом виробництва матеріальних благ і всіх суспільних відносин. Народ – єдине джерело влади, яку він здійснює безпосередньо і через своїх представників – органи влади. Інформованість населення про діяльність органів влади – це невід'ємна умова, що дозволяє суспільству безпосередньо здійснювати владу, контролювати виконання органами держави свого призначення, оцінювати відповідність органів влади інтересам (потребам) особистості й суспільства.

По-перше, предметом інформованості населення є діяльність органів влади, при відсутності нормального громадянського суспільства держава – це та єдина і реальна сила, яка в умовах, що склалися може консолідувати розколоте суспільство, підняти й повести всі його шари й соціальні групи, усі громадські об'єднання на рішення загальнонаціональних завдань із захисту держави і відродження її матеріальної та духовної величі в ім'я рівноправності й рівних можливостей кожного громадянина та кожної сім'ї.

По-друге, від інформованості населення про справи держави, а вони надзвичайно широкі й різноманітні, вирішальною мірою залежать і міцність держави і її здатність виконувати своє призначення, і ставлення населення до своєї держави, й орієнтованість населення на підтримку або неприйняття внутрішньої та зовнішньої політики держави. Зміст цієї інформованості – показник розуміння державою своєї підзвітності населенню, розуміння ролі населення як суб'єкта виробництва й основи суспільних відносин. У глибокій залежності від інформованості населення знаходиться, зокрема, і національна безпека держави, усі її види, у тому числі й інформаційна безпека, безпека особистості та суспільства.

По-третє, інформованість – категорія унікальна. Вона є похідною від однієї з трьох фундаментальних субстанцій (матерія, енергія, інформація), що становлять сутність світобудови. Інформованість як наявність у людей отриманих відомостей,

ідей, фактів, знань, що володіють для них елементами новизни, спонукає споживачів інформації до прийняття відповідних рішень і до адекватних дій. Без інформованості не можуть існувати особистість, суспільство, держава. Це особливо очевидно сьогодні в турбулентних умовах. Під час інформаційного вибуху інформаційний голод, як і дезінформованість – подібні смерті.

Інформованість населення – це результат, досягненням якого підпорядковані інформаційна політика держави та інформаційна культура суспільства, інформаційні технології і системи, інформаційні процеси та процеси інформування. Особливість інформованості як результату полягає і в тому, що вона через своїх споживачів впливає не тільки на інформаційну сферу, а й на всі сфери матеріального та духовного життя людей.

В інформованості відбивається стан, плюси і мінуси збору, зберігання, обробки, передачі та подання інформації її споживачам. Інформованість стає тим засобом (мотивом), який спонукає людей до певних дій. Через інформованість, а точніше через її прояв населенням, правова держава перевіряє свою відповідність призначенню, відповідність своєї внутрішньої та зовнішньої політики, своєї діяльності національним інтересам країни.

У ступені та якості поінформованості населення виявляється і проявляється ступінь корумпованості держави і зрощення її зі злочинним світом, розстановка сил у засобах масової інформації. Інформованість як мета виконує і роль критерію оцінки реальної інформованості, і всього процесу інформування. Інформованість населення як умова і результат, мета і засіб, як характеристика держави, засіб масової інформації може бути і позитивним, і негативним. Інформованість у всіх її ролях стає проблемою тоді, коли отримана споживачем інформація не дозволяє йому безпомилково орієнтуватися, приймати обґрунтовані рішення, коли вона спонукає до збиткових дій.

У найзагальнішому плані суть інформованості як проблеми полягає в її здатності чинити як творчий, так і руйнівний вплив.

У кожному конкретному випадку зміст цієї проблеми може бути свій, специфічний. При цьому не можна не враховувати, що сила, ефективність як творчого, так і руйнівного боку інформованості може домінувати і давати відповідний результат. Інформованість як проблема завжди криє в собі небезпеку для людей у тій сфері, про яку вони отримують інформацію. Природа цієї проблеми – у характері й порядку одержуваної інформації. А спектр їх різноманітності вельми і вельми широкий.

Гострота й актуальність інформованості населення як проблеми інформаційної безпеки постійно вимагають безумовного та ефективного її вирішення. Без цього не можна розраховувати на успіх. Безпечна для держави інформованість населення про діяльність органів влади повинна відповідати ряду вимог:

– Найголовнішою вимогою, якій повинна відповідати інформованість, є обов'язкова адекватність отриманої населенням інформації тим реаліям, які вона відображає. Без цього інформованість спочатку набуває дезінформаційний характер, затуманює свідомість. На превеликий жаль, неадекватність інформації про явища, процеси, предмети стали національним інформаційним лихом. Часто-густо не тільки в побуті, у засобах масової інформації, а й в офіційних документах, у нормативних актах говорять і пишуть одне, а насправді виявляється інше. Ця неадекватність особливо виявляється в змішуванні понять, яке завдає великої шкоди.

– Друга вимога. Інформованість повинна бути повною. Народ, як єдине джерело влади, яку він здійснює безпосередньо та через своїх представників, має право й зобов'язаний мати повну та об'єктивну інформацію про діяльність органів влади, якою б ця інформація не була – гіркою або солодкою, білою або чорною. Тільки повна інформованість гарантує реальну орієнтованість населенню, дає йому можливість приймати обґрунтовані рішення і здійснювати відповідні дії. Повна інформованість не може нашкодити тому, що вона відображає обставини, які обумовлюють необхідність відповідних дій. Якщо наявна інфор-

мація такої необхідності не викликає – вона вже не може вважатися повною.

Крім того, повна інформованість указує на можливі наслідки неприйняття рішень і підказує можливі результати прийнятих рішень. Залежність рішень, дій, вчинків людей від повноти отриманої ними інформації є закономірною, а вимога забезпечення повноти інформованості носить принциповий характер. Значення цієї вимоги неможливо переоцінити. Життя переконливо свідчить, що всі прийняті та реалізовані або нереалізовані рішення, які не дали очікуваних, потрібних результатів, вироблялися без достатньої повноти обізнаності, без прогнозування наслідків їх виконання.

– Третя вимога. Інформованість населення може бути корисною, безпечною для держави, якщо вона буде предметною. Діяльність влади широка й багатогранна. Її багатогранність обумовлена не тільки поділом влади, а й багатопредметністю діяльності кожної з них. Оскільки інформованість – це наявність інформації у людей, яка передбачає прийняття рішень та подальших дій, то вона повинна стосуватися тих предметів діяльності влади, які впливають на сфери матеріального і духовного життя народу. Такими предметами є забезпечення державою реалізації людьми конституційних прав і свобод людини і громадянина, у тому числі і в інформаційній сфері; забезпечення консолідації та підтримання суспільної злагоди; забезпечення органами влади суверенітету й територіальної цілісності, політичної, економічної та соціальної стабільності, законності й правопорядку. Тільки предметна інформованість населення може бути повною, а значить і виконувати свою функцію – спонукати до обґрунтованих рішень і дій.

– Четверта вимога. Інформованість повинна бути не тільки повною, предметною, а й своєчасною. Навіть повна і предметна, але не своєчасна інформованість не може бути творчою.

– І ще одна вимога. Інформованість повинна бути значущою, відповідати інтересам споживачів інформації, незалеж-

но від того, хто вони є, – особистість, соціальна група або суспільство в цілому. Без цього отримана інформація залишиться інертною, що не буде мотивом до рішень і дій.

На жаль, багато дуже важливих для людей подій залишаються за екраном телевізора, за сторінкою газети, за рамками інших засобів інформації. А їхнє місце займає малозначуща, а нерідко й ненависна народу інформація. Зі сказаного випливає, що тільки об'єктивна, повна, предметна, своєчасна та значуща інформованість населення про діяльність органів влади не може бути проблемою інформаційної безпеки держави.

Щоб зробити громадянина досить інформованим для прийняття й реалізації максимально вірного рішення:

– по-перше, від ЗМІ треба очікувати однаково активної роботи від усіх видів масової свідомості (світогляд, світобачення, історична свідомість і особлива громадська думка);

– по-друге, інформування має проходити з урахуванням об'єктивних потреб кожної соціальної групи, соціального прошарку, а також відмінностей в уявленнях, поглядах, настроях;

– по-третє, слід виходити з поняття суспільства як системно організованої цілісності, де кожна група функціонує лише за наявності інших і в органічному зв'язку з ними.

У зв'язку з цим державна (національна) політика в сфері ЗМІ повинна міцно базуватися на ідеї та практиці політичного, ідеологічного, культурного плюралізму, яка передбачає, що всі можливі погляди не тільки можуть, а й повинні бути пред'явлені суспільству, мають бути доступними самим різним верствам, піддаватися всебічному обговоренню з метою пошуку загальноприйнятного рішення. Однак очевидно, що не всі соціальні сили та їхні ідейні представники мають можливість створити свої ЗМІ, а пропоновані в «чужі» ЗМІ матеріали нерідко відкидаються [5]. Результат парадоксальний: замість того, щоб призводити до високої інформованості та злагоди, плюралізм є мало не протилежних цілей.

Основними напрямками державної інформаційної політики є:

• забезпечення доступу кожного до інформації;

• забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

• створення умов для формування в Україні інформаційного суспільства;

• забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

• створення інформаційних систем і мереж інформації, розвиток електронного урядування;

• постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

• забезпечення інформаційної безпеки України;

• сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [6].

Однією зі складових національної політики в сфері ЗМІ повинна бути толерантність – терпимість, притому доброзичлива до поглядів інших, визнаних рівноправними в силу рівності соціальних сил, що їх виражають і захищають. Але просто доброзичливого визнання рівності інших сил і їхніх позицій без активної взаємодії з ними недостатньо. Звідси й необхідність налаштованості на конструктивну взаємодію, хоча потрібно докласти чимало зусиль, щоб виникла свідома солідарність між тими, кого багато розділяє і в позиціях, і в поглядах. У результаті центробіжні тенденції плюралізму, характерні для гуманістичного розвитку суспільства, при вирішенні загальних проблем вимагають активної толерантності, руху назустріч іншому в солідарному прагненні знайти загальноприйнятне рішення. Тому загальнодержавна інформаційна політика повинна включати положення про необхідність активного ведення соціально-

го діалогу в ЗМІ з приводу проблем, до яких по-різному підходять різні соціальні сили.

Способи ведення діалогу можуть бути різними (рис. 3.2.).

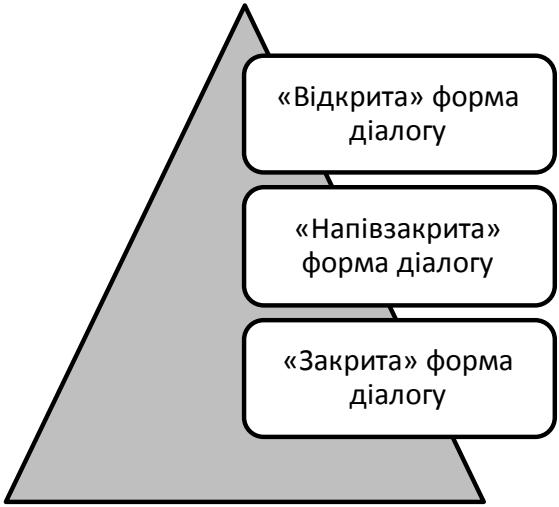


Рис. 3.2. Способи ведення діалогу

«Відкритий» діалог передбачає максимально повний виклад своїх позицій і аргументацій у надії на зустрічну відкритість інших учасників. «Закрита» позиція зводиться до монологічного викладу своєї точки зору при переконаності в її повній правоті [7]. «Напівзакритою» формою діалогу є «монологічний діалог», коли під впливом опонентів вносяться правки до своєї позиції без відкритої вказівки на зроблений «зустрічний крок» і «діалогічний монолог»(при якому взяті до уваги аргументи і пропозиції опонентів вказуються відкрито, однак стверджується, що мова йде про часткову й несуттєву зміну власної позиції).

ЗМІ, що ведуть відкритий діалог, працюють над пошуком такого рішення (компромісу, консенсусу), який був би на користь усім, і не бояться докору від «занадто великих вчинків»

або навіть «втрати обличчя». При цьому зрозуміло: потрібен чіткий і всебічний аналіз проблемної ситуації.

Відкритий діалог, що ведеться однією стороною, у суперечці може наштовхнутися на «закриту» позицію іншої, нерозуміння й небажання йти на зближення та пошук загальноприйнятного рішення, а часом і на прагнення до односторонньої вигоди. Неконструктивна позиція опонента – не привід до «закриття» своєї позиції й переходу на позицію «боротьби до перемоги». Толерантність не повинна заважати тому, хто налаштований на відкритий діалог. Зрештою, незмінність «проблемної ситуації» і бажання однієї сторони знайти вирішення змусить інших стати на шлях відкритого діалогу.

Такі мінімальні вимоги з точки зору МІБ до поведінки ЗМІ. На їхньому фоні реальна картина функціонування ЗМІ дає підстави тривожитися. Аналіз показує, що ряд рис, характерних для ситуації перехідного періоду, вимагає уваги і прийняття необхідних рішень. Ось тільки деякі з них:

– по-перше, це широко лібералізований плюралізм, який реально виявляється в можливості заявляти політичні ідеї та цілі в діапазоні від крайніх правих до ліворадикальних, поширювати інформацію не тільки односторонньо орієнтовану, а й ту, яка ледь прикрито заохочує до насильства, «культу тіла», аморалізму тощо. Існуюче законодавство практично не є перешкодою для «зловживання свободою» ЗМІ, а розпочаті судові справи часто закінчуються нічим і тому не надають стримуючого впливу на інших представників журналістського корпусу, схильних до вільного поводження із законодавчими нормами;

– по-друге, це відсутність широкого, постійного й послідовного моніторингу поведінки ЗМІ з точки зору дотримання того законодавства, яке є, а також відсутність демократично функціонуючих контрольних органів;

– по-третє, незважаючи на збільшення кількості газет, програм ТБ і радіо, можливості громадян отримати необхідну й достатню інформацію не тільки не зростають, а й звужуються.

Прикладом може служити кодування українських телеканалів на супутнику;

– по-четверте, як не дивно, розвиток плюралізму без чітко налагодженого діалогу різних сил і руху до суспільної злагоди із загальнонаціональних проблем призводить до загострення соціальної напруги.

Можна назвати й інші порушення МІБ, процесів і тенденцій. Підсумком їх розвитку виявляється ряд негативних явищ: зниження інтересу до ЗМІ, зменшення тиражів і підписки, недовіра до ЗМІ, падіння їхнього престижу, дезорієнтація суспільства, неясність для багатьох світу, у якому живемо, і «бажаного майбутнього».

3.2. Значення мас-медіа в системі державного управління інформаційною безпекою

Сьогодні ні в кого не викликає сумнівів той факт, що кілька десятиліть тому людство вступило в інформаційну епоху, що зажадала докорінного перегляду основ і підходів у всіх сферах державного управління. Особливого значення в цьому набула проблема забезпечення державної інформаційної безпеки, бо інформаційна сфера охопила практично всі галузі життєдіяльності суспільства.

Розмірковуючи про сучасність, учені, політики, журналісти найчастіше говорять про інформаційне суспільство, підкреслюючи при цьому, що мова йде про нові щаблі суспільного розвитку, де інформаційні технології кардинально змінюють характер організації соціально-виробничих процесів. З'являється так зване двадцятичотирьохгодинне суспільство – глобальна комунікація змушує працювати світову економіку без перерви. А отже, змінюється, безперервно зростає роль масової комунікації та інформації. У зв'язку з цим з'являються нові критерії оцінки рівня цивілізаційного розвитку суспільства, можливості й обсяг інформації, що передається за допомогою електронної

пошти, кількість персональних комп'ютерів, мобільних і фіксованих телефонів. Інакше кажучи, XXI століття у своїх пошуках ресурсів розвитку суспільства спрямоване до нових інформаційно-комунікативних технологій, що забезпечують швидкий і універсальний доступ до інформації.

При цьому ЗМІ як інструмент широкого впливу на маси потребують фільтрації у відборі інформації, що надається суспільству, тому що неперевірена і навіть шкідлива інформація може завдати колосальної шкоди як окремій особистості, так і державі в цілому. Так засоби масової інформації є найважливішим елементом у системі державного управління інформаційної безпеки.

Сучасне інформаційне середовище – це сфера людської життєдіяльності, яка не тільки найбільш динамічно розвивається, але і практично одноосібно диктує умови розвитку сучасного суспільства. Інформаційно-психологічний вплив на людину з боку ІС досить широкий і, у той же час, суперечливий, що викликано турбулентністю сьогодення.

Засобами масової інформації є організації, що створюються для збору, обробки, аналізу інформації та доведення її за допомогою спеціальних технічних засобів до різних соціальних груп [8]. Слід відмітити, що їх основними функціями в сучасних умовах можна назвати наступні: інформативна (надання об'єктивної та неупередженої інформації), захисна (поширення контрпропаганди, захист українського суспільства від маніпуляцій), контрольна (висвітлення роботи державних структур України), культурна (один із базових елементів сталого розвитку громадянської культури української нації) та функція альтернативного джерела інформації (рис. 3.3.) [9].

Цілком можна стверджувати, що реалізація всіх, представлених на рисунку 3.3. функцій, тією чи іншою мірою пов'язані із забезпеченням інформаційної безпеки особистості, суспільства й держави, бо кожна з них несе інформаційну складову, що має значний інформаційний вплив на суб'єктів державності.

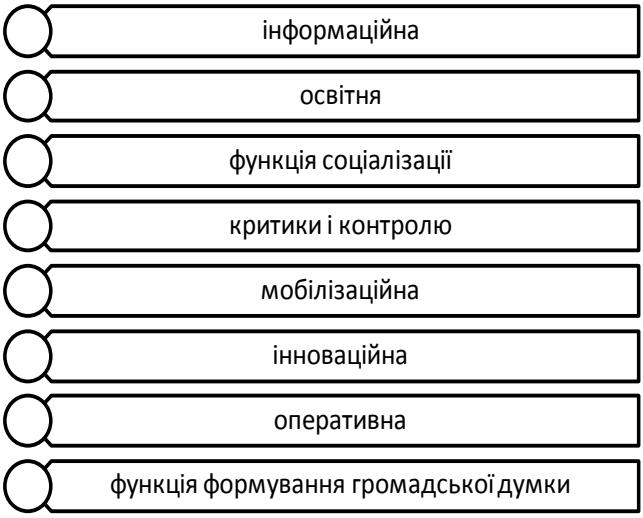


Рис. 3.3. Основні соціальні функції засобів масової інформації

Слід зазначити, що процеси сприйняття глобальним співтовариством імпульсів ЗМІ і закономірностей їх взаємодії з індивідуумами знаходяться в центрі уваги соціологів, а пізніше й політологів уже більше одного століття – з 1920-х років. Нижче наведено історичний нарис даного питання.

На першому етапі дослідження (із 1920 по 1940-і роки) превалював постулат про прямий і блискавичний вплив ЗМІ на суспільну свідомість.

На другому етапі (1940-1960 рр.) була поширена позиція Е. Каца (E. Katz) і П. Лазарсфельда (P. F. Lazarsfeld), які наголосили на важливості врахування соціальних відносин щодо впливу ЗМІ на соціум [10]. Учені довели, що ряд людей-лідерів впливають на поведінку інших через ЗМІ.

На третьому етапі (1960-1980 рр.) дослідники визнали попередні моделі застарілими й почали розробку нової, що від-

повідала вимогам коректного впливу засобів масової інформації на суспільну свідомість.

Сучасний період, початком якого прийнято вважати 80-ті роки XX століття, показав, що єдиної думки вченого співтовариства в досліджуваному питанні немає. Однак превалювати став розроблений ще в класичний період, але не знайшов тоді розуміння, соціально-когнітивний підхід. Майже все, що людський мозок засвоює ззовні, реалізується за допомогою механізму спостереження, в основному за моделями поведінки інших осіб.

Однією з найбільш складних, але в той же час і найдавніших форм подачі інформації є *друк*. Незважаючи на значне падіння попиту на друковану продукцію і значне звуження читацької аудиторії, друковані ЗМІ залишаються практично єдиним загальнодоступним джерелом раціональної, адресної інформації.

До основних особливостей преси можна віднести узагальненість і заглибленість коментарів; аналітичність інтерпретації подій; свободу вибору місця й часу для споживання інформації; можливість повторного звернення до першоджерела.

У пресі найбільш повно реалізується адресність інформації. Так, із достатньою впевненістю можна стверджувати, що на відміну від телебачення й радіо, орієнтованих більшою мірою на усередненого споживача, друковані видання адресовані певній частині аудиторії. Як наслідок, друк виступає в якості засобу ідентифікації читача з тією чи іншою соціальною, регіональною, релігійною спільністю. У цьому плані друковані ЗМІ можна визнати прямим каналом впливу на інформаційну безпеку особистості й окремих соціальних груп.

Разом із тим необхідно звернути увагу на ті особливості друку, які можна віднести до негативних:

- відсутність належної оперативності в поданні інформації;
- заангажованість у подачі інформації та інтерпретації подій;

• достатня дорожнеча видавничої діяльності;

• складність у сприйнятті інформації, яка вимагає певного рівня культури спілкування з друкованим джерелом, освіти, ступеня соціалізованості особистості.

Радіо – переважно фонове джерело інформації, але до сьогодні воно може вийти на перші ролі в поданні інформації в кризові моменти розвитку суспільства, перетворюючись із часом на єдине джерело інформації. Так, необхідно відзначити практику використання радіоприймачів із фіксованими частотами в Алжирі для запобігання повстання частин іноземного легіону, командуванням багатонаціональних сил у Перській затоці для впливу на збройні сили Іраку. Радіо передбачає менше труднощів для виходу в ефір, ніж телебачення, до того ж ці обставини посилюються в умовах монопольного виробництва й передачі інформації, коли полегшений контроль за її змістом. Оперативність радіо та його доступність дозволяє зберігати першість у формуванні початкових установок особистості, що надалі зумовлює формування необхідної громадської думки.

Гіпертрофована публічна політика, пов'язана з пошуком кращого актора, веде до різкого зростання ролі та значення засобів електронної інформації і, перш за все, *телебачення*. У числі специфічних рис телебачення, що відрізняють його від інших ЗМІ, відзначаються:

• доступність його використання в якості джерела інформації;

• доступність сприйняття повідомлення, тому що воно не вимагає особливого освітнього рівня споживача інформації;

• одномоментність події та її відображення, миттєвість;

• полісистемність події, тобто вплив на аудіальну і візуальну систему сприйняття;

• емоційна насиченість інформації, почасти на противагу раціональному початку [11].

Завдяки здатності поширювати аудіо- та відеоінформацію на величезні території, у тому числі, одночасно зі вчинен-

ням події, телебачення сприяє подоланню фізичних бар'єрів у вигляді простору і часу між джерелом інформації та аудиторією. Збагачена наочністю, глядацькою інформацією ця риса телебачення призводить до високої результативності повідомлення, формує в аудиторії інтерес до знання, збільшує її потребу в придбанні більш широкої і глибокої інформації з інших джерел. Тому особливого значення для соціалізації особистості та інформаційної безпеки телебачення і радіо набувають в умовах віддаленості від головних центрів політичного життя й духовного виробництва.

Телебачення, володіючи високою силою наочності, веде до посилення емоційних чинників сприйняття, що підвищує ефективність його впливу на формування установок особистості. Ця якість телебачення створює передумови для більшої переконливості, достовірності телевізійної інформації, у тому числі політичного характеру. Важливе значення має ефект миттєвості, причетності реципієнта до інформації, коли виховання людини здійснюється на матеріалах живих подій. Звідси й роль телебачення в системі джерел зміцнення інформаційної безпеки: за порівняно невеликий час, аж до декількох хвилин, телеглядач отримує велику наочну інформацію, що дозволяє йому самостійно зробити висновки, прийти до якогось рішення, сформувати уявлення та переконання, на що в іншому випадку може знадобитися набагато більше часу [12].

Також зміни в суспільстві відбуваються під впливом *мережевих засобів масової комунікації*. Так, наприклад п'ятдесят років тому, якщо ви захотіли б переслати 30 сторінок тексту на відстань 5 тисяч кілометрів, вам треба було б приблизно 10 днів, і коштувало б це близько 30 доларів за послуги поштового зв'язку. Двадцять років тому ви б, напевно, вдалися до послуг факсу. Це зайняло б у вас приблизно 1 годину, і вартість становила би приблизно 50 доларів. Сьогодні, якщо говорити про найкращі мережі передачі даних, на це потрібно не більше 3 секунд, а вартість складає близько 3 центів. Таким чином, вартість упа-

ла в 1000 разів, швидкість зросла в 300 тисяч разів. Колосальне збільшення швидкості при одночасному зниженні вартості, поява практичної можливості передачі мультимедійної інформації в реальному часі, збільшення швидкості систем пошуку й обробки інформації в мільйон разів це основи майбутнього розвитку всіх сфер життя суспільства.

Однак із іншого боку, розвиток мережевих засобів масової комунікації також не обмежується тільки певними перевагами і вигодами, а й відкриває найширші можливості для ведення інформаційного протиборства в соціально-політичній сфері. Інформаційний тероризм, поширення нелегальних матеріалів утворення в мережі неформальних молодіжних об'єднань, деструктивний вплив нових комунікаційних технологій на особистість – це також атрибут існування мережевих засобів масової комунікації. Поширення Інтернету як у нашій країні, так і в цілому в усьому світі характеризується явною перевагою інтересів бізнесу над інтересами суспільства. Ажіотаж, що склався навколо Інтернету, цілеспрямовано стимулюється комерційними компаніями, що виробляють техніку і програми для Інтернету, а також творцями так званого «інформаційного наповнення». Тим часом досвід «традиційних» засобів масової комунікації показує, що комерційний підхід не здатний задовольнити соціальні потреби суспільства в галузі інформації.

Сьогодні мережеві засоби масової комунікації являють собою нову історичну форму забезпечення взаємодії людей, а Інтернет виступає в якості основи формування єдиного електронного комунікаційного середовища, соціально-політичний сенс якого полягає в можливості створення системи, яка перебуває над національними культурами, цивілізаціями та державами і здатна якісно змінити світ , хоча розширення соціальних функцій системи масової комунікації при цьому не відбувається. Характер і розвиток цього обнадійливого та одночасно небезпечного явища залежить від світових соціальних і політичних процесів і, у

свою чергу, має на них певний вплив (зокрема, загострює й динамізується).

Отже, у наш час інформаційно-технічного прогресу стає цілком очевидним, що Інтернет може виявитися не тільки засобом обміну інформацією, діалогічного спілкування й розваги, а й, як усі інші ЗМІ, може використовуватися як засіб впливу та маніпулювання.

Однією з проблем, безпосередньо пов'язаних з інформаційною безпекою, є здатність і реальна можливість ЗМІ маніпулювати свідомістю людини й громадською думкою. Наприклад, усебічно описані характеристики комунікатора, що сприяють підвищенню ефективності людської мови, зокрема, виявлено типи його позиції під час комунікативного процесу. Таких позицій може бути три: відкрита, відсторонена та закрита (рис. 3.4).

Рис. 3.4. Типи позиції під час комунікативного процесу

Природно, що зміст кожної з позицій, що представлені на рис. 3.4, задається метою, завданням, яке переслідується в комунікативній дії, але важливо, що принципово кожна з названих

позицій стає певною можливістю для підвищення ефекту впливу. Таким чином, будь-яка людина отримує разом із самим індивідуальним повідомленням, ще й коментар.

Практично коментар є маніпуляцією. Слід зазначити, що до маніпуляції відносяться спеціальні дії формування стереотипів і створення певного враження або ставлення до того чи іншого факту, події. Основний об'єкт впливу коментаря-маніпуляції – це матриці свідомості української політичної еліти й усього українського населення. Способи маніпулювання громадською думкою спираються, перш за все, на засоби масової інформації, що дозволяють коригувати, регламентувати й проєктувати масову свідомість і психіку людей. При цьому акцент робиться на використання законів психології, некритичне сприйняття, політичну недосвідченість.

Аналіз зарубіжних і вітчизняних джерел свідчить про те, що способи, які застосовуються для обробки громадської думки за допомогою ЗМІ, у різних країнах багато в чому ідентичні. У цілому маніпулювання засноване на брехні й омані. Основою для маніпулювання служать міфи (фактично – дезінформація).

У політичній науці сформувалося два основних підходи, що характеризують ступінь впливу ЗМІ на політичний процес. Вони мають деяку схожість за своїм змістом із історичною класифікацією етапів розвитку ЗМІ.

Прихильники першого підходу вважають, що ЗМІ мають серйозний вплив на громадян і їхні політичні орієнтації. Так, наприклад, П. Бурдьє вважає, що ЗМІ є головним інструментом «обдурення» мас [13]. Теоретичною базою для прихильників цього наукового підходу є праця У. Ліппма «Громадська думка», яка вийшла у 1922 р. У ній автор, розглядаючи участь ЗМІ в електоральних процесах США, довів, що ЗМІ всесильні у формуванні політичних уподобань населення. Надалі, у 1960-і роки, ця концепція була доповнена Б. Коеном, який розробив теорію і дав визначення особливого ефекту ЗМІ, що дозволяє управляти інформаційними хвилями і відповідно темами тих чи інших

політичних дискурсів. Він дав назву цьому феномену «ефект порядку денного», тим самим розвинув і вдосконалив роботу У. Ліппман. Його теза полягала в тому, що ЗМІ не можуть спонукати маси думати певним чином, але цілком реально можуть позначити тему для роздумів (люди думають, як хочуть, але ось те, про що вони думають, визначено за них) [14].

Прихильники другого підходу, навпаки, применшують ступінь прямого впливу ЗМІ на реципієнта через низку опосередкованих факторів. Вони вважають, що ЗМІ всього лише дають людині інформацію про політичний світ, не торкаючись її індивідуальних політичних уподобань. Раніше згаданий П. Лазарсфельд, аналізуючи вплив ЗМІ на президентських виборах у США в 1940-х роках, стверджував, що інформація, передана виборцю по каналах ЗМІ, лише підсилює вже існуючі установки й орієнтації [10].

Ці орієнтації сформувалися під впливом таких чинників, як соціальний статус, професія або добробут. Крім того, П. Лазарсфельд увів до наукового обігу «двоступеневу» модель комунікації. Відповідно до цієї моделі ЗМІ формують оцінки поточних подій не в усієї цільової групи, а тільки в невеликої її частини, кількістю не більше 10%. Рефлексивне переосмислення інформації відбувається лише в меншості, яка найбільше схильна до цього процесу. Лазарсфельд назвав таких людей «лідерами думок», які передають своє розуміння поточної ситуації іншим громадянам, що менше цікавляться політичним процесом [10].

Слід зауважити, що як прихильники, так і опоненти версії значного впливу ЗМІ на політичний процес не можуть виключити зі сфери розгляду політичного процесу самі ЗМІ, а сперечаються лише про ступінь їхнього впливу на свої аудиторії, не намагаючись спростувати існування такого впливу.

У сучасному світі інноваційних технологій інформаційна безпека вже зараз є соціальним і тільки потім чисто технічним явищем. Її не можна ототожнювати лише із застосуванням спеціальних технічних засобів і методів для захисту інформації

від несанкціонованого доступу, викрадення, знищення тощо, як зазначалося раніше, це необхідний комплекс заходів організаційного та правового характеру, спрямованих на забезпечення сталого, стабільного розвитку суспільства й держави.

Також система міжнародної інформаційної безпеки покликана протидіяти загрозам стратегічної стабільності і сприяти рівноправному стратегічному партнерству в глобальному інформаційному просторі [11]. Основними ризиками в галузі міжнародної інформаційної безпеки можуть стати використання інформаційних та комунікаційних технологій:

• у якості інформаційної зброї у військово-політичних цілях, що суперечать міжнародному праву, для здійснення ворожих дій і актів агресії, спрямованих на дискредитацію суверенітету, порушення територіальної цілісності держав і становлять загрозу міжнародному миру, безпеці і стратегічній стабільності;

• у терористичних цілях, у тому числі для надання деструктивного впливу на елементи критичної інформаційної інфраструктури, а також для пропаганди тероризму та залучення до терористичної діяльності нових прихильників;

• для втручання у внутрішні справи суверенних держав, порушення громадського порядку, розпалювання міжнаціональної, міжрасової й міжконфесійної ворожнечі, пропаганди расистських і ксенофобських ідей або теорій, що породжують ненависть і дискримінацію, які підбурюють до насильства.

Протистояння інформаційним ризикам можливе при дотриманні виконання наступних напрямків:

• розробка дієвих організаційно-правових механізмів доступу засобів масової інформації та громадян до відкритої інформації;

• забезпечення достовірності відомостей про соціально значимі події суспільного життя, які розповсюджуються через ЗМІ;

• недопущення підпорядкування ЗМІ кон'юнктурним інтересам влади й бізнесу та посилення можливостей їхнього

впливу на ЗМІ (прямий натиск, постачання ЗМІ неповної, невизначеної, спотвореної або помилкової інформації, відвертої дезінформації, умисних недомовленостей, зрощування структур влади, бізнесу, преси тощо);

• регулювання рівня концентрації та монополізації ЗМІ (перешкоджання зменшенню незалежних джерел інформації, зосередження ЗМІ в руках представників економічної еліти, безправ'я журналістів тощо);

• удосконалення національного законодавства в частині гарантій свободи слова та інформації, вільне поширення масової інформації, у тому числі на транскордонному рівні, недопущення поширення насильства й нетерпимості через ЗМІ, забезпечення плюралізму ЗМІ, доступ до офіційної інформації.

Інформаційному середовищу притаманне постійне та стрімке розширення. Особливо бурхливе розширення інформаційного середовища суспільства відбувається останнім часом, і темпи його постійно зростають. За таких умов особистості дуже складно розібратися в якості й істиності отримуваної інформації, що створює дезорієнтацію не тільки в інформаційному полі, але й у реальності.

Постійне оновлення ІС призводить до того, що люди навіть не встигають формулювати власну думку з приводу подій, що відбуваються, тому швидше сприймають уже готову інтерпретацію, запропоновану постачальником інформації, що негативно позначається на здатності сучасних людей до аналітичного, критичного мислення, і, як наслідок, у них знижується «імунітет» до маніпулятивного впливу.

Використання ЗМІ об'єктивно передбачає залежність національної безпеки держави від захищеності інформаційного середовища. Це багато в чому визначає ступінь уразливості національного інформаційного простору перед впливом недружніх держав, терористичних організацій, кримінальних спільнот і окремих осіб, що діють через інформаційний простір.

Як уже відзначалося, ЗМІ перетворилися на «четверту» владу, від якої багато в чому залежать зміни, що відбуваються в суспільстві. Саме тому проблема створення систем інформаційної безпеки держави є настільки актуальною на сучасному етапі.

Засоби масової інформації разом із органами державної влади можуть і повинні брати участь у забезпеченні інформаційної безпеки таким чином, щоб процес циркуляції інформації не переривався, інформація не спотворювалася, а права та інтереси її суб'єктів не обмежувалися.

Серед основних напрямків державного регулювання інформаційної безпеки є розробка дієвих організаційно-правових механізмів, забезпечення достовірності відомостей про соціально значимі події, недопущення підпорядкування ЗМІ, регулювання рівня концентрації та монополізації ЗМІ, удосконалення національного законодавства в частині гарантій свободи слова та інформації, вільного поширення масової інформації, у тому числі на транскордонному рівні.

Першочерговість стратегії інформаційної безпеки держави полягає в подоланні турбулентності й досягненні чіткої керованості. Необхідна систематизація та алгоритмічне використання механізмів задля забезпечення внутрішньої інформаційної безпеки і формування підтримки України в суспільствах країн-партнерів. Необхідний комплексний характер актуальних ризиків національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту й розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

3.3. Засоби масової комунікації як платформа забезпечення державної інформаційної політики в сфері цифрової трансформації суспільства

Державна інформаційна політика – важливий аспект державного управління в інформаційному суспільстві. Існують різні інститути, через які реалізуються заходи державної інформаційної політики. До них можна віднести інститути зв'язку з громадськістю, аналітичні центри, інститути культури. Однак базовим механізмом реалізації державної інформаційної політики служать засоби масової інформації. Саме вони здатні створювати інформаційний порядок, що відіграє найважливішу роль при формуванні громадської думки.

На сьогоднішній момент украй важливо приділяти увагу розвитку державної інформаційної політики, яка виступає системоутворюючим фактором, що впливає на побудову конструктивного діалогу між владою і суспільством.

На сучасному етапі розвитку суспільства зростає роль інформаційної сфери, що в сукупності представляє собою інформаційну інфраструктуру, суб'єктів, які збирають, формують, розповсюджують і використовують інформацію, а також системи, що регулюють при цьому суспільні відносини. Інформаційна сфера є системоутворюючим фактором життя суспільства й активно впливає на стан різних галузей життя держави.

Із розвитком технологій і швидкості передачі даних у постіндустріальному суспільстві збільшується роль і значення інформації та засобів масової інформації. Це визначило необхідність створення державами системи управління в галузі інформації або державної інформаційної політики.

У даний час державна інформаційна політика повинна бути найважливішою складовою зовнішньої і внутрішньої політики країни, а побудова демократичного інформаційного суспільства і входження країни у світове інформаційне співтовариство є довгостроковою стратегічною метою. Причинами цього є

стрімкий розвиток інформаційного суспільства та глобалізація медійного простору, а також настання епохи інформаційних війн і протистояння в боротьбі за вплив на громадськість.

Будь-якій державі завжди були потрібні певні ресурси для підтримки своїх рішень, дій, реформ, які забезпечували б найбільш адекватний і бажаний їх супровід і прийняття з боку громадян цієї держави. Раніше це не складало особливих труднощів через певну в цьому плані простоту державного функціонування: рішення, по суті, просто декларувалися населенню, а інструментом, що забезпечує супровід державних дій, була сама форма державного устрою. Це форма правління, коли кроки, що застосовуються державою, просто не прийнято було обговорювати серед простих громадян. До того ж, із найдавніших часів стійкість політичної системи будь-якої держави залежала від того, наскільки швидко й повно політична еліта отримувала інформацію та наскільки швидко на неї реагувала. У результаті аналізу інформації про зміни в зовнішньому середовищі політичні еліти вживали заходів щодо збереження стійкості політичної системи своєї держави.

Однак із плином часу участь громадян (звичайно, не всіх, а з певних соціальних груп), а вірніше, їхні думки, судження про підготовку в державі змін, тих чи інших кроків у внутрішній або зовнішній політиці стали набувати певної ваги. Правлячі кола, чини держави поступово стали потрапляти в якусь залежність від громадської думки це впливало на їхню особисту популярність і можливість подальшої роботи на своїх державних посадах.

Стає очевидним, що в суспільно-політичному житті держави (поряд із повсякденним життям кожної людини) усе більшого значення набуває інформація як така, а отже, і засоби, які володіють цією інформацією і транслюють її. У сучасному суспільстві ступінь інформатизації, розвитку різних каналів підготовки, отримання, передачі тих чи інших зведень, новин досягла, можна сказати, своєрідного піку в плані залежності від них навіть

простого щоденного побуту людей. Інформація перетворилася на глобальний, у принципі невичерпний ресурс людства, що вступив у нову епоху розвитку цивілізації – епоху інтенсивного освоєння інформаційного ресурсу.

Однак важливим є той факт, що володіння тією чи іншою інформацією змінює не тільки уявлення людей про якісь буденні речі. Певним чином подана інформація впливає на думку громадськості в набагато більш важливому й масштабному вимірі у сфері суспільних, економічних і політичних відносин. Із розвитком інформатизації суспільства засоби масової комунікації починають надавати все більш відчутний вплив на різні сфери життя соціуму, зокрема на політичну свідомість і поведінку населення. Отже, особливо важливого значення набуває те, звідки та чи інша інформація надходить, як вона формується і подається, поширюється в суспільстві й доходить до своїх адресатів - конкретної соціальної чи електоральної групи або, наприклад, громадян інших держав. Йдеться, безумовно, про засоби масової інформації, які виступають не тільки як інструмент об'єктивної передачі новин, але і як основний їх творець.

ЗМІ в сучасному світі відіграють у політичному житті суспільства істотну роль (якщо не одну з визначальних), маючи безпосереднє відношення до його життєдіяльності і виконуючи репродуктивну (відображають політику через радіо, телебачення і пресу) і креативну (яка творить) функції.

Основною причиною завоювання ЗМІ настільки високого місця в політичному житті сучасних суспільств є те, що з їх допомогою держава й інші політичні суб'єкти можуть не тільки інформувати населення про цілі та цінності своєї політики, а й моделювати відносини із громадськістю, що стосуються формування представницьких органів влади і правлячих еліт, підтримання авторитету відповідних цілей, традицій і стереотипів [15]. Інакше кажучи, ЗМІ стали найпотужнішим інструментом цілеспрямованого конструювання політичних порядків, засобом вибудовування необхідного владі зв'язку і відносин із громадськістю.

Основна роль ЗМІ на даний момент не стільки інформаційна, скільки ідеологічна, тобто ЗМІ не стільки транслюють інформацію, що відображає об'єктивний стан суспільних настроїв, скільки виступають інструментом, який ці настрої формує, направляє за допомогою певної інформації.

По суті, зараз політику й політичну діяльність можна охарактеризувати як інформаційну боротьбу за вплив на думки, судження політичної еліти, соціальних груп і міжнародної громадськості. Поведінку людських колективів можна і формувати, задаючи певні орієнтири шляхом тонких психологічних маніпуляцій. Сучасні ЗМІ створили для цього принципово нові можливості, багаторазово посиливши ефективність використання інформації в політичних цілях [16]. Вони зробили справжню революцію у політичних відносинах і способах соціального управління світом. Так, у XX ст. володіння й управління інформаційними потоками перетворюється на вирішальний фактор завоювання, збереження, утримання влади.

Виходячи з теорії, також однією з найважливіших функцій ЗМІ є безпосередній вплив на владу, владні структури. Різні журналістські роботи з викриття несумлінних чиновників, сумнівних державних рішень і законопроєктів, винесених на суд громадськості, дають підставу вважати, що ЗМІ дійсно здатні впливати на державні органи влади, служачи тим самим «рупором» громадськості. Засоби масової інформації не тільки створюють докладну картину політичного життя, установлюють «повістку дня» [17], привертають увагу до діяльності різних політичних акторів, формують ціннісні установки громадян, а й контролюють спрямованість політичної активності різних соціальних спільнот і груп. Однак реальна практика традиційно має свої розбіжності з теорією, а саме: у сучасному суспільстві очевидна наявність взаємодії держави й засобів масової інформації, саме держава виступає замовником і контролером інформації, поширюваної через ЗМІ.

Якщо повернутися до тези про те, що зі зростанням ролі демократичних віянь і цінностей у сучасному суспільстві (свобода слова, вибору, активну участь громадян у державному житті і їхню можливість міняти розстановку політичних кадрів держави та ін.) кожній державі необхідно мати суспільну підтримку своїх реформ і кроків як у внутрішній, так і у зовнішній політиці, неминуче постає питання про взаємодію влади та засобів масової інформації.

У результаті проведеного аналізу сучасних наукових підходів, інформаційна політика визначається як здатність і можливість суб'єктів політики впливати на свідомість, психіку людей, їхню поведінку й діяльність у своїх інтересах за допомогою інформації. Такий підхід виносить поняття інформаційної політики в площину ідеологічної боротьби, зближуючи його з пропагандою. У західній політичній науці склався інший підхід до розуміння державної інформаційної політики, який вказує на переважаюче значення інтересів суспільства. Ключовими елементами процесу здійснення інформаційної політики є ідентифікація інформаційних потреб суспільства, розробка засобів задоволення цих потреб, стимулювання ефективного використання інформаційних ресурсів. Але такий підхід характерний тільки для держав із сильним громадянським суспільством, а значить, його не завжди можна застосувати.

Під державною інформаційною політикою в сучасних умовах слід розуміти систему заходів, реалізованих органами державної влади, спрямованих на підтримку єдності і збереження контролю над інформаційним простором за допомогою інформаційного впливу та використання інформаційних технологій. Суб'єктом інформаційної політики є держава в особі різних структур і органів державної влади. Об'єктом виступає інформаційна сфера суспільства. Інформаційна сфера являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють виробництво, збір, зберігання, поширення і ви-

користання інформації, а також системи регулювання суспільних відносин, що виникають при цьому.

Виходячи з цього, можна виділити напрямки, на які слід зробити акцент для здійснення грамотної державної інформаційної політики у сучасних реаліях:

• розвиток громадянського суспільства;

• забезпечення конструктивного діалогу між державою, ЗМІ та суспільством;

• визнання презумпції відкритості інформації для громадян і захист їхніх інформаційних прав;

• орієнтацію головних компонентів інформаційного простору на забезпечення вільного обігу інформації, утілення в життя конституційного права на вільний пошук, отримання, виробництво інформації та її поширення;

• підвищення довіри суспільства до влади;

• налагодження ефективних взаємовідносин держави на міжнародній арені тощо.

При цьому варто відзначити, що засоби масової комунікації одночасно служать об'єктом, на який спрямована особлива увага органів державної інформаційної політики як на один із найважливіших механізмів її реалізації. Існують різні інститути, через які реалізуються заходи державної інформаційної політики [18]. Наприклад, до них можна віднести інститути зв'язків із громадськістю, аналітичні центри, інститути культури. Однак базовим механізмом реалізації державної інформаційної політики є засоби масової інформації.

ЗМІ, привертаючи увагу аудиторії до певних тем, створюють у свідомості споживачів інформації картину світу, яка може відрізнятися від соціальної реальності. Ця картина світу є гнучкою, яка коригується і грає найважливішу роль у формуванні громадської думки. При цьому створювана повістка не стає автоматично пріоритетом аудиторії, а також не означає формування однозначної консолідованої позиції за освітлюваними темами. Засоби масової інформації через повторюваність, де-

талізацію, час і місце, відведене тій чи іншій темі, визначають її значимість для аудиторії.

Сутність інформаційної повістки полягає в тому, що засоби масової інформації представляють аудиторії деякі проблеми, які є найбільш важливими на даний момент. Зазвичай їх виділено не більше п'яти. При цьому важливо розуміти, що повістка (порядок денний) не має прямого впливу на поведінку індивідів. Вплив масової комунікації на аудиторію завжди опосередкований міжособистісною і внутрішньогруповою комунікацією. При цьому одночасно можуть існувати кілька повісток, наприклад, інформаційна, внутрішньогрупова, міжособистісна. У той же час політична повістка також може поділятися на рівні (національна, регіональна, місцева).

Традиційні засоби масової інформації поділяють за способом передачі інформації на електронні, друковані та поширювані в мережі Інтернет. Проте за рівнем керованості найдоцільніше розділяти засоби масової інформації на державні та недержавні. Недержавні засоби масової інформації можуть контролювати юридичні та фізичні особи або іноземні юридичні і фізичні особи. Усе різноманіття ЗМІ, що існує і здійснює свою діяльність на території країни, являє собою медіасистему. У рамках даної системи ЗМІ займають різне становище й мають різний вплив на інформаційну повістку в залежності від безлічі факторів.

На жаль, основний вплив на зміст і політику видань надає власник, інтереси й позицію якого представляє ЗМІ. Також величезний вплив на місце ЗМІ в системі медіа надає охоплення мовлення. ЗМІ можна розділити на три категорії:

1) транслюються по всій території країни;

2) регіонального рівня;

3) глобальна мережа Інтернет.

ЗМІ хоча і є інструментом реалізації державної інформаційної політики, проте діють на різних рівнях і вимагають різних підходів до управління.

Таким чином, суб'єктом державної інформаційної політики є органи влади. Спосіб взаємодії суб'єктів інформаційної політики та ЗМІ значною мірою залежить від політичного режиму і способу, моделі поширення інформації, що склалася в державі. Дані відносини можна розділити на кілька моделей залежно від типу політичного режиму, переважної форми власності ЗМІ та їхньої політичної позиції (рис. 3.5.):

Рис. 3.5. Моделі поширення інформації залежно від типу політичного режиму

– *тоталітарна*, передбачає жорсткий диктат із боку держави по відношенню до всіх об'єктів інформаційної сфери без винятку;

– *плюралістична*, передбачає наявність опозиційних, а також приватних, недержавних структур, що діють у даній сфері;

– *тоталітарно-плюралістична*, при якій ідеологічне різноманіття номінально присутнє, у той же час актори (індивід, соціальна група, організація, інститут, спільність людей), дії яких суперечать позиції держави, великого впливу не мають;

– *олігархічно-плюралістична*, при якій розповсюджувачі інформації відстоюють інтереси бізнес-еліт і приватних корпорацій, а не держави або суспільства, зі збереженням видимості функціонування інститутів демократії. При цьому держава не має контролю над інформаційним простором.

У цілому механізми управління засобами масової інформації даних рівнів можна розділити на адміністративно-правові та інформаційні.

До адміністративно-правових відносяться:

• механізми реєстрації ЗМІ, у тому числі отримання ліцензій на мовлення;

• правове регулювання інформації, що розміщується у ЗМІ (наприклад, заборона на розміщення матеріалів, що містять заклик до міжетнічної ворожнечі);

• економічні форми впливу, у тому числі пряме фінансування й контракти на надання інформаційних послуг, гранти на окремі проєкти, державні субсидії;

• контроль економічної діяльності з боку силових структур, тобто контроль економічної діяльності засобів масової інформації як суб'єктів бізнесу (наприклад, при сплаті податків, економічної діяльності).

До інформаційних можна віднести:

– доступ до інформації, присутність на офіційних заходах, можливість оперативного отримання інформації, у тому числі ексклюзивної;

– доступ до інформації про поточну діяльність органу влади;

– наближеність до керівників структур, можливість отримання коментарів та інтерв'ю перших осіб;

– якість інформації, яка транслюється для ЗМІ.

Способи маніпулювання громадською думкою, як реальна частина зовнішньої і внутрішньої політики держави, повністю спираються на засоби масової інформації, що дозволяють коригувати, регламентувати і проєктувати в масовій свідомості громадян певне ставлення до тих чи інших подій, державних намірів і дій.

Маніпуляція громадською думкою є однією з найсерйозніших проблем сучасного політичного життя: методи, що використовуються в політичній пропаганді, є серйозною загрозою психічному здоров'ю, особливо ясному та критичному мисленню, емоційній незалежності. Проте незважаючи на потенційно небезпечні наслідки інформаційного впливу за допомогою ЗМІ, можна все ж з упевненістю констатувати, що в даний час відбулися й остаточно зміцнилися в арсеналі сучасної політики принципи інформаційного впливу, інструментом якого виступають засоби масової інформації, до яких кожен громадянин звертається сотні й тисячі разів щодня.

Засоби масової інформації формують інформаційний порядок і відіграють найважливішу роль для створення громадської думки. Цей факт визначає особливе значення ЗМІ як механізму реалізації державної інформаційної політики. Існує ряд факторів, таких як, наприклад, форма фінансування, територія мовлення, політичні позиції власників ЗМІ, які визначають положення засобів масової інформації в медіасистемі та здатність їх задавати інформаційну повістку.

Засобам масової інформації, як джерелу інформаційної безпеки, необхідно вести свою інформаційну політику, виходячи з вимог МІБ:

1. Усі громадяни повинні бути надійно забезпечені повною, достовірною, оперативною інформацією, що дає кожному із соціальних суб'єктів можливість гранично всебічно й максимально об'єктивно, відповідно до своїх потреб, положенню в суспільстві орієнтуватися в дійсності (факти, оцінки, норми, ідеали) і приймати оціночні й поведінкові рішення, адекватні ситуації в

конкретній сфері (світі, регіоні, країні, місті, районі), аж до міжособистісних відносин на роботі, у сім'ї тощо.

2. Має діяти стільки загальнодоступних каналів масової інформації та в такому розмаїтті, що це дозволило б зробити такий вибір ЗМІ, який відповідає потребам соціального суб'єкта.

3. Різноманітність має стосуватися позицій, які подаються з тим, щоб кожен міг познайомитися з усіма варіантами й самостійно, усвідомлено, максимально вірно визначити свою позицію, виходячи з власних інтересів і прагнень.

4. Кожен із соціальних суб'єктів у відповідності зі своєю позицією і цілями повинен мати можливість поширювати від власного імені і в своїх інтересах масову інформацію, у тому числі створювати (засновувати, співзасновувати, субзасновувати) ЗМІ та мати юридичні, економічні та інші можливості вільно шукати, отримувати, компонувати інформацію в номери (випуски, програми).

5. На виступи, запитання, репліки кожного суб'єкта має бути гідна, обґрунтована, «адресна» реакція тих, кому їх адресовано, і/або від тих, хто зацікавлений у виробленні чітких і переконливих поглядів у суспільстві щодо обговорюваної проблеми. Адже якщо когось «не чують» і замість відповіді «мовчать», то формування необхідних інформаційних ресурсів даного суб'єкта виявляється під ударом.

6. Кожен соціальний суб'єкт має право розраховувати на отримання регулярної можливості відстоювати свою позицію, спростовувати погляди опонента, відкрито шукати спільними зусиллями загальноприйнятну або прийнятну для більшості точку зору, рішення обговорюваної проблеми в загальнонаціональних інтересах; «свобода критики» всіх повинна бути звільнена від популізму, демагогії та інших прийомів дезорієнтації.

7. Необхідна максимальна відкритість джерел інформації й доступність їх для всіх громадян, а також розвиток прес-служб різних установ, відомств тощо.

8. Усі споживачі масової інформації (і соціальні інститути, й окремі громадяни) повинні накопичувати та реалізовувати навички роботи з потоками масової інформації різної спрямованості. У такому «вихованні» аудиторії визначальна роль належить самим ЗМІ, які, демонструючи свої підходи й обґрунтовуючи їх, критикуючи опонентів, шукаючи через діалог рішення обговорюваних проблем, тим самим «вчать» аудиторію розбиратися в хитросплетіннях інформаційного протиборства. Саме ЗМІ несуть основну відповідальність за формування особистісних і громадянських якостей, здатних протистояти інформаційним ризикам.

Основними напрямками інформаційної політики у сфері ЗМІ повинні стати:

• Недопущення підпорядкування ЗМІ кон'юнктурним інтересам влади й бізнесу та посилення можливостей їхнього впливу на ЗМІ (прямий натиск, постачання ЗМІ неповною, невизначеною, спотвореною або неправдивою інформацією, відвертою дезінформацією, умисних недомовленостей, зрощування структур влади, бізнесу, преси тощо);

• Регулювання рівня концентрації та монополізації ЗМІ (перешкода зменшенню незалежних джерел інформації, зосередження ЗМІ в руках представників економічної еліти, безправ'я журналістів тощо);

• Захист інтересів регіональних ринків масової інформації та сприяння розвитку місцевих ЗМІ;

• Удосконалення національного законодавства в частині гарантій свободи слова та інформації, вільного поширення масової інформації, у тому числі на транскордонному рівні, недопущення поширення насильства й нетерпимості через ЗМІ, забезпечення плюралізму ЗМІ, доступу до офіційної інформації.

Для успішного здійснення державної інформаційної політики потрібно скоригувати ряд моментів:

• необхідно вдосконалити законодавчу базу у сфері ЗМІ та засобів масової комунікації з можливістю широкого обговорення законопроєктів;

• сформувати суспільні комісії скарг на ЗМІ;

• заснувати інститут омбудсменів у ЗМІ;

• розробити систему економічної підтримки друкованих ЗМІ для реалізації плюралізму думок і підвищення якості видань, а також розширення кола читачів за рахунок зниження вартості друкованих видань;

• створити систему екології ЗМІ;

• стимулювати формування системи етичного регулювання діяльності преси.

Список використаних джерел

1. Панченко О.А., Антонов В.Г., Гуменюк В.В. Информационная безопасность личности в условиях изменяющихся социокультурных ценностей. Вісник Одеського національного університету. Серія: Психологія. 2016. №. 21. Вип. 2. С. 140-149.

2. Панченко О.А. Информационно-психологическая безопасность в условиях гражданского противостояния. Психология стресса и совладающего поведения: ресурсы, здоровье, развитие: материалы IV Междунар. науч. конф. Кострома. 22–24 сент. 2016 г.: в 2 т. отв. ред.: Т.Л. Крюкова, М.В. Сапоровская, С.А. Хазова. Кострома: КГУ им. Н. А. Некрасова. 2016. Т. 2. – С. 311-314. URL: https://www.elibrary.ru/item.asp?id=27718187 (дата звернення 08.05.2020).

3. Панченко О.А. Інформаційна безпека держави як елемент соціальної культури. Аспекти публічного управління. 2020.№ 1.Том 8.С. 58-67. URL: https://aspects.org.ua/index.php/journal/article/view/720/692 (дата звернення 08.05.2020).

4. Панченко О.А. Засоби масової інформації як джерело інформаційної безпеки. Експерт: парадигми юридичних наук і державного управління.2020. № 2(8) С. 250-258. DOI: 10.32689/2617-9660-2020-2(8)-250-258. URL: http://maup.com.ua/assets/files/expert/8/21.pdf (дата звернення 08.07.2020).

5. Панченко О.А. Роль засобів масової інформації в системі державного управління інформаційною безпекою. Пу-

блічне управління та митне адміністрування. 2020. № 1(24). С. 97-102. DOI: 10.32836/2310-9653-2020-1.19. URL: http://customs-admin.umsf.in.ua/archive/2020/1/19.pdf (дата звернення 08.07.2020).

6. Закон України «Про інформацію» від 02.10.1992 року № 2658-XII [Редакція від 03.12.2019 р.];. Сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 08.05.2020).

7. Панченко О.А. Засоби масової комунікації як платформа державної інформаційної політики. Державне управління: удосконалення та розвиток. Київ. № 4. 2020. DOI: 10.32702/2307-2156-2020.4.2. URL: http://www.dy.nayka.com.ua/pdf/4_2020/4.pdf (дата звернення 08.05.2020).

8. Панарин И.Н. Информационная война и власть. М: Издательский дом «Мир безопасности». 2001. С. 100.

9. Головка А.А. Діяльність сучасних ЗМІ в контексті інформаційної безпеки України. «Актуальні проблеми гуманітарних та природничих наук» (м. Ужгород. 08-09 квітня 2016 р.). Херсон. Видавничий дім «Гельветика». 2016. С. 85-87

10. Katz E., Lazarsfeld, P. (1955) Personal Influence: The Part Played by People in the Flow of Mass Communication. Glencoe, IL : The Free Press.

11. Панченко О.А., Банчук Н.В. Информационная безопасность личности. 2-е изд. испр. К.: КИТ. 2011. 672 с.

12. Почепцов Г. Логика пропаганды, или Новости без грима. Media Sapiens. 2015. URL: http://osvita.mediasapiens.ua/trends/1411978127/logika_propagandy_ili_novosti_bez_grima/ (дата звернення 08.05.2020).

13. Майофис М., Кукулин И. Свобода как неосознанный прецедент: заметки о трансформации медийного поля в 1990 году. М. Новое литературное обозрение. 2007. № 83. С. 599-656.

14. Осипова Н. Г., Юрченко Е. И. Средства массовой информации в современном обществе: теоретико-методологи-

ческий анализ новейших подходов М. Вестник Московского университета. Сер. 18. Социология и политология. 2010. №1. С. 64–85.

15. Торяник В.М. Інформаційна безпека як складова національної безпеки держави, роль ЗМІ в забезпеченні інформаційного суверенітету України. Право і суспільство. 2016. №2. С.151-156.

16. Дьякова Е.Г. Массовая коммуникация и власть. Екатеринбург. УрО РАН. 2002. 299 с.

17. Бритков В.Б., Дубовской С.В. Информационные технологии в национальном и мировом развитии. Общественные науки и современность. 2000. № 1. с. 146-150

18. Панченко О.А. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. Серія: Державне управління. 2019. Випуск 3. URL: http://77.222.145.174/index.php/governance/article/view/296/297 (дата звернення 08.05.2020).

РОЗДІЛ 4

Засади формування системи державного управління у сфері інформаційної безпеки дитини в Україні

4.1. Інформаційні ризики безпеки дитини в турбулентному інформаційному середовищі

У розділі 2 було наголошено, що ризик – це можливі події, явища і процеси, наслідки яких можуть мати несприятливий вплив на різні аспекти стану людського життя (у тому числі й на інформаційну безпеку). Подібне трактування має і поняття «загроза». Різниця полягає в тому, що загроза – це ймовірна можливість завдання шкоди, а ризик вимірює, оцінює цю загрозу, дає уявлення щодо конкретного виразу ймовірності завдання шкоди. У той же час загроза – це пасивне явище, яке потенційно може перетворитись на активне (дію) – вплив. Небезпека – це конкретнаформа прояву загрози, створена впливом, деструктивний характер якої є цілком усвідомленим та беззаперечним.

Можна стверджувати, що ступінь загрози та її перехід у форму небезпеки характеризується рівнем ризику, який, у свою чергу, визначається ймовірністю настання та впливом на особистість. Тобто за прийнятного рівня ризику негативний вплив факторів зовнішнього та внутрішнього середовища розглядається як загроза особистості, а за досягнення критичного рівня ризику загроза приймає форму небезпеки.

Викладені сентенції дозволяють трактувати інформаційні ризики безпеки дитини в турбулентному інформаційному середовищі як сукупність умов, факторів та явищ, під дією яких можливе порушення стану інформаційної безпеки дитини, її психологічного стану або створення небезпеки її життєво важливим інтересам.

В.М. Фурашев зазначає, що інформаційна загроза – це з одного боку такий внутрішній чи зовнішній інформаційний

вплив, що створює небезпеку зміни напрямку, темпів прогресивного розвитку індивідуумів чи суспільних утворень, а з іншого боку – це небезпека для останніх стати жертвою негативного інформаційного впливу [1].

Під негативним впливом стосовно дитини слід розуміти «таку дію інформації або дію за допомогою інформації з використанням спеціальних засобів і технологій, яка завдає шкоди фізичному чи психічному здоров'ю дитини або спонукає її до девіантної поведінки» [2]. Поряд із поняттям «інформаційний вплив» використовується й «інформаційно-психологічний вплив», оскільки він пов'язаний із втручанням у внутрішній психологічний та психічний стан дитини через її свідомість та підсвідомість, із використанням інформаційних технологій, що призводить до негативних і деструктивних наслідків для дитячої психіки.

Дитяча психіка дуже вразлива по відношенню до інформаційних впливів унаслідок несформованості найважливіших психічних функцій і структур, що забезпечують адекватну переробку інформації і психологічний захист особистості. Спираючись на соціальні контексти розвитку, внутрішню позицію дитини і її ставлення до світу, інформаційна безпека дитини (ІБД) повинна враховувати два аспекти: захист від негативного впливу інформаційного середовища й розвиток умов, що забезпечують позитивну соціалізацію та індивідуалізацію дитини [3]. Тобто, *інформаційна безпека дитини – це захищеність від негативного впливу інформаційного середовища на здоров'я, психічний, духовний, моральний розвиток; створення умов для позитивної соціалізації особистості, оптимального особистісного розвитку, збереження соматичного, психічного та психологічного здоров'я і благополуччя, формування позитивного світосприйняття.*

Топчій О.В. у межах поняття «інформаційна безпека дитини» пропонує диференціювати інформаційну безпеку малолітніх і неповнолітніх [4]. Можна погодитись із такою думкою, якщо

розглядати малолітніх і неповнолітніх у якості відособлених учасників інформаційно-правових відносин. Топчій О.В. аргументує це, насамперед, тим, що молода людина, яка вже відійшла від специфіки малолітніх, але ще не набула повною мірою дієздатності, має вікові, психологічні, фізіологічні, соціально-поведінкові особливості. Слід також враховувати, що на сучасному етапі процеси правової соціалізації особистості, зокрема кіберсоціалізації, супроводжуються ментальним протиборством в аксіологічній системі координат, випробуванням навірність обраних ідеологем, а то й суттєвим послабленням морального «імунітету» під впливом медіасфери. Наявність первинних знань у галузі інформаційних технологій, широке розповсюдження ґаджетів у побуті нерідко підштовхують неповнолітніх до перших спроб вчинення інформаційних правопорушень, що може призводити до зміни статусу особи від потенційної жертви шкідливої інформації до джерела інформаційних загроз.

У цьому руслі Н.В. Ортинська підкреслює: «існують розбіжності у відносинах, у які неповнолітні можуть вступати самостійно нарівніз дорослими суб'єктами права, та особливими відносинами, які не визнають неповнолітнього повноцінним суб'єктом права» [5].

Топчій О.В. пропонує під інформаційною безпекою неповнолітніх розуміти *захищеність (як ціль, стан, процес і результат) особи, яка знаходиться на етапі своєї соціалізації й неповної дієздатності, від негативного впливу інформаційного середовища на основі системного застосування науково обґрунтованого комплексу адміністративно-правових, організаційно-управлінських, технологічних і психолого-педагогічних засобів і з метою забезпечення її права на інформацію та сприяння безперешкодному розвиткові й самореалізації особистості.*

Порівнюючи це визначення з вищенаведеним щодо дитини, можемо побачити їх суттєву схожість, окрім доповнення «на основі застосування…».

В обох дефініціях можна помітити особливості, які відрізняють дитину (неповнолітнього) від абстрагованої особистості в інформаційній безпеці, а саме те, що вона ще не завершила етап у своїй соціалізації та не набула повної дієздатності. Тим самим підкреслюється уразливість молодої людини й важливість забезпечення державою і суспільством інформаційно-захисної функції. З урахуванням масового охоплення неповнолітніх інформацією через медіапростір, соціальні мережі, засоби комунікації негативний вплив ІС може викликати ризики на рівні національної безпеки держави.

Радзієвська О.Г. розділяє ризики та загрози для дитини на індивідуальні та суспільні [6]. Індивідуальні – це такі ризики й загрози, що викликані інформаційними впливами, направленими на індивідуальну свідомість та підсвідомість дитини, які можуть призводити до деструктивних наслідків, негативно впливати на формування особистості, її фізичне, психічне чи моральне здоров'я та викликати девіантну поведінку. Суспільні – це такі ризики й загрози, що викликані інформаційними впливами, спрямованими на суспільну свідомість, які можуть призвести до дисбалансу в суспільних відносинах, порушити суспільні норми та викликати девіантну поведінку дитини в соціумі через дію деструктивного інформаційного пливу на її індивідуальну свідомість, що призводить до формування хибних світоглядних позицій, видозмінених моральних, етичних та загальнолюдських цінностей і порушення її комунікативних навичок.

Виявлення загроз в ІС має свої труднощі через ряд причин, серед яких:

– заподіяння шкоди відбувається в ментальному просторі;

– практично неможливо визначити ступінь заподіяння шкоди;

– ступінь заподіяння шкоди залежить від індивідуальних психофізичних особливостей людини та її емоційно-психологічного стану;

– настання наслідків заподіяння шкоди відтерміновано в часі;

– визначення деяких загроз можливе лише постфактум, після виявлення наслідків діяння;

– не існує єдиного інструментарію виявлення загроз, лише опосередковані методи комплексного аналізу психофізичного, суспільно-політичного та інформаційно-технічного чинників.

При розгляді властивостей ІС (див. Розділ 2) акцентовано увагу на тому, що великі обсяги інформації, що циркулюють в ІС, змінюють як саму людину, так і сутність суспільних відносин. Щодо дитини, то вона не спроможна зосередити увагу на конкретній тематиці, відбуваються психофізичне виснаження, утомленість та зміни емоційного стану (збудження чи загальможення). Відсутність належного рівня концентрації уваги разом із мозаїчністю (кліповістю) подачі інформації сучасними засобами передачі інформації (телебачення, Інтернет) призводить до поверхневого її сприйняття, і це може призвести до зниження інтелектуального рівня дитини, її вміння аналізувати, зіставляти, оцінювати, узагальнювати та використовувати інформацію. У протидії негативним інформаційним впливам такі вміння можуть бути недостатніми, особливо у випадку цілеспрямованих маніпулятивних дій на свідомість дитини.

ІС не завжди пропонує істинні цінності, а підміняє їх на систему символів та ілюзорних норм. Прикладом такої підміни понять є реклама, особливо – політична, де істина підміняється чарівним образом, створюється ілюзія позитиву та приховується інший його бік. Через відсутність аналітичних фільтрів дитина такі образи сприймає як істинні та вбудовує їх у власну систему поглядів та цінностей. У подальшому ці образи будуть служити їй як еталонні. Це призведе до видозміни свідомості дитини, викривлення її світосприйняття та основних цінностей. Дитина з видозміненою свідомістю, вступаючи в суспільні відносини, змінюватиме й саме суспільство.

Другим фактором, що несе суттєву загрозу для формування особистості в дитини, є *медіанасилля*, яке впливає на свідомість та підсвідомість дитини. Беззаперечним є й той факт, що збільшення агресії на екрані провокує підвищення агресивної поведінки дитини в реальному житті, а відтак – збільшення агресії у суспільстві [7]. Слід також звернути увагу й на агресивні комп'ютерні ігри, що становлять загрозу не лише психологічному, але й фізичному здоров'ю дитини та викликають залежність. Діти, які часто грають в агресивні комп'ютерні ігри, не до кінця усвідомлюють нереальність подій у грі і, перебуваючи у стресовій ситуації під дією психологічного навантаження, можуть переносити здобуті тут навички в реальне життя. Зважаючи на заохочення в іграх убивства призами й подарунками, у дитини створюється хибне враження, що насилля – це добре. Це значно спотворює у неї уявлення про основні моральні цінності [8].

Найбільш небезпечним, на наш погляд, є вплив соціальних мереж. У визначенні інформаційної безпеки дитини було виділено однією зі складових створення умов інформаційного середовища для позитивної соціалізації та індивідуалізації особистості.

Відомо, що соціалізація відбувається впродовж усього життя людини, при цьому традиційні форми соціалізації включають два види – первинну і вторинну. Первинна соціалізація відбувається з дитинства в межах родинних зв'язків, вторинна – у межах соціальних інститутів і соціальних контактів поза межами безпосереднього життєвого середовища людини [9]. І саме соціальні мережі все більше впливають на вторинну соціалізацію людини. Під впливом мережевого суспільства змінюється стиль життя людей, зокрема звичні канали отримання інформації, характер міжособистісних взаємин, структура дозвілля, відбувається інтенсивне вироблення нових моделей взаємодії з середовищем. Безумовно, усе це впливає на безперервний процес соціалізації молодої людини. Більш того, Інтернет є не

тільки потужним агентом вторинної соціалізації, але й виграє конкуренцію в інститутів, які реалізують первинну соціалізацію. Цьому сприяє динаміка сучасного життя, криза традиційних інститутів і цінностей.

Як відомо, будь-яка діяльність спрямована на задоволення потреб. Спеціально проведені дослідження дозволили визначити певне коло потреб, які підлітки задовольняють за допомогою соціальних мереж та Інтернету, а саме:

– потреба в самостійності (у процесі соціалізації ця потреба припускає, у першу чергу, прагнення до незалежності від батьків);

– потреба в самореалізації та визнанні (зазвичай підліткам украй необхідно відчувати себе особливими та необхідними);

– потреба в пізнанні та визнанні (молоді люди хочуть відчувати себе важливою частинкою певної групи й суспільства загалом);

– задоволення соціальної потреби в спілкуванні, у приналежності до групи за інтересами, у любові, адже підлітковий період – це час, коли людина прагне знайти схожих собі за інтересами, уподобаннями;

– потреба у володінні (підліток має на меті бути обізнаним з усіма подіями, що відбуваються навколо нього);

– пізнавальна потреба (володіння новими знаннями сприяє досягненню визнання з боку однолітків і самореалізації);

– у результаті використання соціальних мереж виникає відчуття повного контролю і володіння ситуацією, що задовольняє потребу в безпеці – одну з базових у системі потреб людини (цитується за [10]).

Завдяки соціальним мережам підлітки проявляють свою індивідуальність, тільки вже не стандартними способами, закладеними процесом перетворення від індивіда до сталої особистості, а завдяки комп'ютерним технологіям.

Дані статистики за 2018 рік показують ([11-13]):

– 95% дітей віком від 13 до 18 років мають постійний доступ до смартфонів, і 45% із них говорять, що знаходяться онлайн «практично завжди»;

– 88% підлітків спостерігали в соцмережах, як хтось був злим або жорстоким по відношенню до іншої людини;

– 67% підлітків знають, як приховати від батьків те, чим вони займаються в соцмережах;

– 66% дорослих користувачів Facebook не мають поняття, як користуватися налаштуваннями конфіденційності;

– 55% батьків, які мають дітей 12 років і молодше, відповіли, що їхні діти вже зареєстровані в Facebook. Більш того 76% відсотків із них самі допомогли в цьому дітям;

– 41% підлітків уже мали негативний досвід у соцмережах;

– 29% дітей спілкувалися в соціальних мережах із незнайомими людьми;

– 29% сексуальних злочинів мають передісторію в соціальних мережах;

– 22% підлітків заходять до улюблених соцмереж не менше 10 разів на день;

– 25% – зіткнулися в реальному житті з проблемами через те, що написали у своїх постах, у 6% це викликало труднощі в школі;

– 22% підлітків утратили друзів через свої дії у соцмережах;

– тільки 10% дорослих розмовляли «по душам» зі своїми дітьми 10 років і менше про безпечну поведінку в соціальних мережах.

Безперечно, використання соцмереж, як джерела нової інформації, інструмента самовираження, спілкування, має певні плюси. Але якщо дорослі, можуть фільтрувати інформацію, то з дітьми зовсім інша історія. Їхня психіка не «загартована». Поспілкувавшись у соцмережах, діти можуть відчувати себе емоційно спустошеними, відчувати депресію. Крім того, спілку-

ючись здебільшого через месенджери, а не обличчям до обличчя, діти не можуть навчитися розпізнавати емоції співрозмовника і зчитувати мову тіла, вираз обличчя й інтонацію, тобто вони втрачають невербальну частину інформації.

Формування більш слабких соціальних навичок спілкування не єдина небезпека, яка може спіткати на дитину в соціальних мережах.

Спам, віруси, фішинг. Небажані послання рекламного характеру з підозрілими посиланнями можуть з'являтися як в коментарях, так і в особистих повідомленнях. Причому, в адресанта часто значаться знайомі профілі: спамери зламують чужі акаунти, щоб робити масові розсилки друзям їхніх власників. Часто спамери створюють фейкові акаунти, що дублюють уже існуючі, щоб подружитися, втертися в довіру, а потім виконати свою місію – закидати непотрібною інформацією, заманити на свій сайт або спонукати скачати документ. Поширені види спаму:

– реклама будь-яких товарів або послуг;

– повідомлення про виграш у лотерею або отримання спадщини;

– лист щастя / нещастя;

– прохання підтвердити дані;

– привабливі пропозиції грошового заробітку;

– прохання позичити грошей або допомогти фінансово.

Тролі. Так називають тих, хто залишає коментарі з певною метою – спровокувати конфлікт або яскраву емоційну реакцію (викликати злість або гнів). Тому тональність їхніх висловлювань завжди недоброзичлива, це цілком може бути безглуздий жарт про маму, критика творчості дитини або її зовнішності, перебріхування фактів і т.ін. Зазвичай коментарі тролів жодним чином не пов'язані з контентом, під яким їх написали. Тролі рідко постять і залишають коментарі від свого особистого імені. Привілей тролів – анонімність, а значить, однією з причин тролінгу може бути бажання висловити те, що дитина не змогла б висловити знайомому безпосередньо. Можливо, він давно її ображає

в реальному житті – у дворі або школі. Інша причина тролінгу може полягати в тому, що діти 12-17 років тільки-тільки починають приміряти на себе соціальні ролі, і нехай не завжди їхній вибір можна назвати раціональним, тролінг у мережі здається їм нешкідливим (на рівні «приколу» або «Пранк»).

Хейтери. Хейтерами називають у соцмережах тих, хто всіляко намагається нівелювати заслуги успішних людей. Чужі невдачі радують хейтера більше, ніж власний успіх. Принижуючи інших, вони самоствердуються. Серед причин, чому користувачі стають хейтерами, часто називають такі:

– їх засмучує, що в іншої дитини є те, чого немає в них;

– вони вважають, що дитина не гідна популярності й слави, яку має;

– у минулому в них з цією дитиною був конфлікт або, навпаки, дружні відносини, які погано закінчилися;

– вони заздрять;

– їм не вистачає уваги та любові.

Кібербулінг. В основному кібербулінг характерний для дітей 12-17 років, саме вони найчастіше використовують Інтернет для залякування, переслідування, погроз або приниження своїх однолітків. Ознаки кібербулінгу:

– в особистих повідомленнях у соцмережах безліч загроз від одного або кількох людей за короткий проміжок часу;

– дитині приходять повідомлення від соцмереж, що на неї поскаржилися за неприйнятну поведінку (скаржиться відразу кілька людей, щоб зробити дитину ізгоєм навіть у соцмережах);

– її відзначають у постах, де опубліковані принизливі фотожаби, відео, образливі жарти, жорстокі хештеги;

– в акаунта дитини з'явився клон, який агресивно поводиться по відношенню до інших користувачів і таким чином псує репутацію дитини;

– у соцмережах поширюється контент, який висміює дитину, її зовнішній вигляд або поведінку.

Групи смерті. Це такі онлайнквести в соціальних мережах, із якими пов'язують кілька смертей підлітків 15-16 років в Україні та Росії (синій кит, Момо і т.ін.). Дітям пропонують виконувати різні завдання – від цілком «невинних» (типу підйом о 4.20 ранку або перегляд фільмів-жахів) і до таких екстремальних, як нанесення собі каліцтв і самогубство.

Підсумовуючи, варто підкреслити ще одну особливість. Діти дуже безпечні щодо інформації про членів родини, дозвілля, оприлюднення персональних даних, спілкування з незнайомцями. Це створює сприятливі умови для використання соціальних мереж із злочинною метою. Крім цього, акаунт будь-якого користувача також може містити різністатистичні дані перебування користувача в мережі: дату, час, тривалість, адреси, використані при підключенні комп'ютера та ін. Тобто, кожен акаунт – це сховищеперсональних даних і повний архів листування. Більшість користувачів навіть не здогадуються про те, наскільки широкому колу осіб конфіденційна інформація може стати відомою, не усвідомлюють реальну й потенційну небезпеку можливого протиправного використання відповідним чином аналітично обробленої їхньої персональної інформації щодо фактично всіх сфер їхнього особистого життя.

Немає сумнівів у тому, що дитина, будучи активним учасником суспільних відносин в інформаційній сфері, є найбільш незахищеним їх суб'єктом у силу вікового онтогенезу та підвищеної інформаційної вразливості, тому вона потребує особливого захисту з боку держави.

4.2. Міжнародні нормативно-правові документи щодо забезпечення інформаційної безпеки дитини

Інформаційна безпека дітей є предметом регулювання великої кількості міжнародних актів. При цьому під час вирішення протиріч між забезпеченням прав і свобод дорослих осіб та захистом прав і законних інтересів дітей, пов'язаних із забезпе-

ченням їхнього здоров'я та розвитку, застосовуються такі принципи [3]:

– допустимість обмеження законом свободи слова, масової інформації та художньої творчості з метою поваги прав і репутації інших осіб, охорони державної безпеки, громадського порядку, здоров'я і моральності населення;

– реалізація диференційованого підходу в законодавчому забезпеченні прав і свобод дорослих і неповнолітніх, який передбачає введення більш жорстких стандартів захисту прав дітей, у порівнянні із захистом прав дорослих;

– пріоритетність прав та інтересів дітей, їхньої моральності, здоров'я, фізичного, розумового, духовного й соціального розвитку, забезпечення державою особливогоїхнього захисту як найбільш вразливої групи.

Міжнародні стандарти інформаційної безпеки дітей, у першу чергу, передбачають:

– розробку й закріплення спеціальних заходів протидії демонстрації невмотивованого насильства, поширення матеріалів, що містять зображення жорстокості, порнографії та інші небезпечні для молоді види інформації у формі електронних ЗМІ, відеозаписів та ін.;

– виключення показу дітей і особистих відносин у формі, що принижує гідність;

– припинення й попередження будь-якого зловживання зображенням або голосом дитини в еротичних цілях.

Базовим міжнародним актом у сфері прав людини є «Загальна декларація прав людини», прийнята 10 грудня 1948 року Генеральною Асамблеєю ООН [14]. У числі основних прав людини в ній закріплені:

– право на свободу думки, совісті й релігії, включаючи свободу змінювати свою релігію або переконання і свободу сповідувати свою релігію або переконання як одноособово, так і спільно з іншими, публічним або приватним порядком у нав-

чанні, богослужінні і виконанні релігійних та ритуальних обрядів (ст. 18);

– право на свободу переконань і на вільне їх виявлення, включаючи свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати й поширювати інформацію та ідеї будь-якими засобами незалежно від державних кордонів (ст. 19).

Разом із тим, закріплюючи зазначені права, Декларація передбачає допустимість їх обмеження: «При здійсненні своїх прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які встановлені законом виключно з метою забезпечення належного визнання й поваги прав і свобод інших та задоволення справедливих вимог моралі, громадського порядку й загального добробуту в демократичному суспільстві» (ст. 29).

У сфері правового забезпечення захисту прав людини особлива увага приділяється стандартам у галузі прав дитини, оскільки діти є пріоритетним об'єктом захисту від негативного інформаційно-психологічного впливу. Базовим універсальним документом у цьому відношенні є «Конвенція ООН про права дитини» від 20 листопада 1989 р. [15], спрямована на забезпечення інтересів дитини й обов'язки держав «забезпечити дитині такий захист і піклування, які необхідні для її благополуччя, беручи до уваги права й обов'язки її батьків, опікунів або інших осіб, котрі відповідають за неї за законом», для виконання якої вони «вживають усіх відповідних законодавчих і адміністративних заходів» (ст. 3).

Стаття 12 Конвенції зобов'язує держави забезпечити дитині, здатній сформулювати власні погляди, право вільно висловлювати ці погляди з усіх питань, що торкаються дитини, причому поглядам дитини приділяється належна увага згідно з її віком і зрілістю.

У статті 13 гарантується право дитини на свободу вираження своєї думки, що включає право на свободу шукати, одержувати й передавати інформацію та ідеї будь-якого роду, неза-

лежно від кордонів, в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів за вибором дитини.

Конвенція також закріплює право дитини на свободу думки, совісті й релігії (ст. 14). При цьому обумовлюється, що «держави-учасниці поважають права та обов'язки батьків і у відповідних випадках законних опікунів керувати дитиною у здійсненні її права методом, що відповідає здібностям дитини». Документ закріплює також ряд принципів, що стосується захисту дітей від ряду кримінальних загроз (ст.19), а також гарантує право дитини на захист від економічної експлуатації (ст. 32), а також від будь-яких інших форм експлуатації (ст. 36).

Особлива увага приділяється захисту дітей від сексуальної експлуатації та сексуального розбещення. Із цією метою держави-учасники, зокрема, уживають на національному, двосторонньому та багатосторонньому рівнях усіх необхідних заходів для запобігання: а) схиляння або примусу дитини до будь-якої незаконної сексуальної діяльності; б) використання з метою експлуатації дітей у проституції або в іншій незаконній сексуальній практиці; в) використання із метою експлуатації дітей у порнографії та порнографічних матеріалах (ст. 34).

Важливе значення в контексті проблеми інформаційної безпеки дітей має стаття 17 Конвенції, у якій мова йде про роль ЗМІ у взаємодії з дітьми. Згідно з цією статтею, «держави-учасниці визнають важливу роль засобів масової інформації і забезпечують, щоб дитина мала доступ до інформації і матеріалів із різних національних і міжнародних джерел, особливо до такої інформації і матеріалів, які спрямовані на сприяння соціальному, духовному й моральному благополуччю, а також здоровому фізичному й психічному розвитку дитини». Разом із тим передбачається обов'язок держав уживати заходів щодо захисту дитини від негативної інформації, що завдає шкоди її благополуччю.

Постановою Верховної Ради України № 789XII (78912) від 27 лютого 1991 року Конвенція була ратифікована та набула чинності для України 27 вересня 1991 року.

2 березня 2016 року Комітетом міністрів Ради Європи була прийнята «Стратегія Ради Європи з прав дитини (2016 – 2021 рр.)», де серед п'яти пріоритетних напрямків діяльності для гарантування прав дитини відповідно до викликів сьогодення визначено забезпечення прав дитини в цифровому середовищі [16].

У документі вказується (п. 58), що Рада Європи буде заохочувати й захищати права дітей на захист від дискримінації, доступ до інформації, свободу вираження думок і участі в цифровому середовищі у співпраці з іншими зацікавленими сторонами, що діють у цій галузі. Будуть розроблятися та розповсюджуватися додатки для смартфонів і планшетів, а також інші засоби комунікації для розширення можливостей дітей, батьків і педагогів і безпечного використання потенціалу ІКТ і цифрових медіа. Спираючись на рекомендації з питань політики підтримки позитивного батьківства та інші відповідні стандарти, будуть розроблені керівні принципи щодо виховання дітей у цифрову епоху, засновані на правах дитини.

Рада Європи буде стимулювати, контролювати й підтримувати здійснення заходів, що забезпечують міцну основу для захисту дітей від потенційних ризиків для їхньої безпеки та конфіденційності в цифровому середовищі (п. 59).

Універсального документа щодо ЗМІ, норми якого були б юридично обов'язковими для всіх держав, не існує. Відправнезначення мають уже згадані вище документи, а також «Міжнародний пакт про громадянські й політичні права», прийнятий резолюцією 2200 А (XXI) Генеральної Асамблеї від 16 грудня 1966 року [17], які гарантують право на свободу переконань і на вільний їх вираз, включаючи свободу шукати, одержувати й поширювати інформацію та ідеї будь-якими способами та незалежно від державних кордонів. Свобода масової інформації

розглядається як одна зі складових названого основного права людини безперешкодно дотримуватися своїх поглядів. У зв'язку з цим на неї поширюються норми міжнародних актів про права людини, що стосуються допустимості обмеження свободи вираження думок у певних цілях, а також містяться заборони пропаганди геноциду, апартеїду, расової дискримінації, поширення інформації, яка збуджує расову, національну чи релігійну ненависть і ворожнечу.

Останні питання більш детально відображені в «Декларації про основні принципи, що стосуються внеску засобів масової інформації у зміцнення миру й міжнародного взаєморозуміння, у розвиток прав людини й у боротьбу проти расизму й апартеїду та підбурення до війни» від 28 листопада 1978 року [18], прийнятої Генеральною конференцією ЮНЕСКО на її двадцятій сесії. У Декларації наголошується, що ЗМІ повинні вносити важливий вклад у зміцнення миру й міжнародного взаєморозуміння і в боротьбу проти расизму, апартеїду й підбурювання до війни (ч. 1 ст. III). Для цього в документі регламентовані позитивні заходи, яких повинні вживати ЗМІ для досягнення цілей, зазначених у назві Декларації. Так, згідно з ч. 2 ст. III «у боротьбі проти агресивних воєн, расизму, апартеїду та інших порушень прав людини, які є, поряд з іншим, породженням забобонів і невігластва, засоби інформації, поширюючи відомості про ідеали, прагнення, культуру й потреби всіх народів, сприяють ліквідації невігластва та нерозуміння між народами, усвідомлення громадянами однієї країни потреб і прагнень інших, забезпечення поваги прав і гідності всіх націй, усіх народів і всіх осіб, незалежно від раси, статі, мови, релігії чи національності, і привернення уваги до таких великих лих людства, як злидні, недоїдання і хвороби, сприяючи, таким чином, виробленню державами політики, що найбільш сприяє ослабленню міжнародної напруженості й мирному і справедливому врегулюванню міжнародних суперечок».

У рамках Ради Європи прийнято велику кількість конвенцій і декларацій, присвячених свободі масової інформації. Пра-

вовою підставою для них є стаття 10 про свободу вираження поглядів «Конвенції про захист прав людини й основних свобод» (Європейська Конвенція із прав людини, ЄКПЛ [19]).

Одним із таких документів є «Декларація про засоби масової інформації і права людини» від 23 січня 1970 року [20], яка закріплює дві найважливіші норми:

1. Незалежність преси та інших засобів масової інформації від державного контролю повинна бути записана в законі. Будь-яке обмеження цієї незалежності допускається тільки на підставі рішення суду, а не органів виконавчої влади.

2. Не повинно бути ні прямої, ні опосередкованої цензури преси або змісту радіо-телевізійних програм, новин або інформації, що передаються іншими засобами, наприклад, хронікальних матеріалів, що демонструються в кінотеатрах. Обмеження можуть накладатися в межах, дозволених статтею 10 ЄКПЛ.

Одночасно документ закріплює ряд вимог до самих ЗМІ. Перш за все, підкреслюється, що преса й інші ЗМІ зобов'язані виконувати свої функції із почуттям відповідальності перед суспільством і окремими громадянами. Для реалізації цього передбачається ряд заходів, включаючи прийняття кодексу професійної етики для журналістів і здійснення самоконтролю самими ЗМІ, де за основу повинні бути віднесені наступні положення:

а) поширення точних і збалансованих повідомлень, виправлення неправильної інформації;

б) проведення чіткої різниці між поширюваною інформацією і коментарями;

в) недопущення поширення наклепницьких тверджень;

г) повагу права на особисте життя.

Ще одним важливим документом є «Декларація про свободу вираження поглядів та інформації» від 29 квітня 1982 року [21]. У документі підкреслюється важливість свободи вираження поглядів та інформації для демократії й поваги прав людини та закріплюється обов'язок держав охороняти цю свободу від порушень, а також здійснювати політику, спрямовану

на підтримку якомога більшої різноманітності засобів інформації і множинності джерел інформації, допускаючи, таким чином, плюралізм ідей і думок. Декларація підтверджує такі цілі держав в області інформації та ЗМІ, як охорона права кожного на вільне вираження думки, пошук та отримання інформації незалежно від державних кордонів, відсутність цензури й будь-яких довільних контрольних механізмів або примусу по відношенню до учасників інформаційного процесу, змісту засобів інформації або при передачі або розповсюдженні інформації, існування широкої різноманітності незалежних і автономних засобів інформації, що допускають відображення різноманітності ідей і думок та ін.

Розглянуті декларації Ради Європи носять рекомендаційний характер. На відміну від них, «Європейська конвенція про транскордонне телебачення» від 5 травня 1989 року [22] є обов'язковою для виконання. Конвенція ставить за обов'язок телемовника здійснення контролю за тим, щоб програми в цілому, їх уявлення і зміст забезпечували повагу до гідності людської особи та основні права інших людей. Зокрема, вони не повинні: а) бути непристойними і, особливо, містити порнографію; б) неправомірно пропагувати насильство. Усі програми, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків, не повинні транслюватися в той період часу, коли вони можуть їх дивитися (ст. 7). Відповідно до даної Конвенції реклама, адресована дітям або виконана з їх використанням, не повинна завдавати шкоди їхнім інтересам і зобов'язана враховувати їхню особливу сприйнятливість (ст. 11).

У рамках політики Європейського Союзу в цій сфері в якості основного використовується таке джерело права, як *директиви,* в яких указано цілі й результати, що підлягають досягненню, при наданні національним властям права самим визначати механізм їх виконання. Крім того, у даній сфері прийнято ряд рекомендацій ЄС, які мають значення керівних орієнтирів для національних органів влади. Основою для прийняття даних актів виступає стаття 3 «Договору про Європейський Союз» (за ре-

дакцією Лісабонського договору від 13 грудня 2007 року) [23], яка проголошує захист прав дітей у якості однієї з цілей діяльності ЄС.

Основним документом ЄС у сфері мас-медіа тривалий час була Директива Ради ЄС 89/552 / ЄЕС від 3 жовтня 1989 року, відома як Директива «Телебачення без кордонів» (Television wit hout Frontiers Directive) [24]. У даному акті містилася спеціальна глава 5: «Захист неповнолітніх і громадського порядку», а також інші норми, спрямовані на захист неповнолітніх, що передбачають заборону реклами тютюнових виробів (ст. 13), обмеження на рекламу алкогольних напоїв (ст. 15); вимогу про неприпустимість заподіяння рекламою фізичного або морального збитку неповнолітнім (ст. 16).

У 2007 році прийнята Директива 2007/65/ЕС28, що вносить поправки до Директиви «Телебачення без кордонів» і трансформує її в Директиву про аудіовізуальні медіа послуги (Audio visual Media Services Directive). 10 березня 2010 року прийнята кодифікована версія даної директиви [25]. У новій редакції документ поширив свою дію на аудіовізуальні послуги, що надаються провайдером для перегляду програм за вибором глядача (on-demand). У ньому частково збережені колишні й закріплений ряд нових норм, що стосуються захисту неповнолітніх. Так, ст. 9 Директиви закріпила норму, згідно з якою держави-учасниці гарантують, що аудіовізуальні комерційні комунікації не завдаватимуть фізичної й моральної шкоди неповнолітнім. Тому вони не будуть безпосередньо пропонувати неповнолітнім придбати товар або скористатися послугою, використовуючи їхню недосвідченість або довірливість, безпосередньо підбурювати їх умовляти своїх батьків або інших осіб придбати рекламовані товари або послуги, використовувати особливу довіру неповнолітніх до батьків, учителів або інших осіб, або невиправдано зображувати неповнолітніх у небезпечних ситуаціях.

Директива зберегла спеціальну главу (7) про захист неповнолітніх у телевізійному мовленні, оновивши її зміст порівняно

з попередньою Директивою і представивши її в такій редакції (ст. 27):

1. Держави-учасниці будуть дотримуватись відповідних заходів для забезпечення того, щоб передачі телемовників, які перебувають під їхньою юрисдикцією, не включали програми, що можуть завдати серйозної шкоди фізичному, духовному й моральному розвитку неповнолітніх, зокрема програми, що містять порнографію або невиправдане насильство.

2. Заходи, передбачені в пункті 1 цієї статті, повинні також поширюватися на інші програми, які можуть порушити фізичний, духовний та моральний розвиток неповнолітніх, за винятком тих випадків, коли за допомогою вибору часу трансляції або застосування спеціальних технічних засобів, що виключають можливість перегляду або прослуховування неповнолітніми таких передач.

3. Крім того, коли такі програми транслюються в некодованій формі, Держави-учасниці повинні гарантувати, що їм буде передувати звукове попередження або наявність візуального попередження протягом усієї трансляції».

Незважаючи на актуальність проблеми, що стосується забезпечення інформаційної безпеки дітей у мережі Інтернет, суспільні відносини в цій сфері ще не отримали комплексного правового регулювання ні на загальному, ні на регіональному рівнях. Тут домінують переважно політико-декларативні документи, тоді як міжнародних договорів із жорсткими юридичними зобов'язаннями практично немає.

Одним із найбільш відомих документів є «Окінавська Хартія глобального інформаційного суспільства» від 22 липня 2000 року [26]. У документі в частині безпеки підкреслюється, що зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, повинні супроводжуватися «узгодженими діями щодо створення безпечного і вільного від злочинності кіберпростору» (ст. 8).

За підсумками Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства в Женеві була прийнята Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» від 12 грудня 2003 року [27], що представляє собою досить об'ємний і комплексний документ. Поряд із іншими аспектами в ньому приділено увагу питанням довіри і безпеки при використанні ІКТ. У якості основного напрямку вирішення цих завдань називається формування, розвиток і впровадження глобальної культури кібербезпеки (ст. 35). Женевська декларація приділяє увагу й етичним аспектам інформаційного суспільства (розділ 10). У ній визнається значимість етичних норм, що повинні сприяти справедливості, а також підтримувати гідність і цінність людської особистості. Для цього всі учасники інформаційного суспільства повинні «робити відповідні дії і приймати встановлені законодавством заходи щодо запобігання неналежного використання ІКТ, такого як незаконні та інші дії на ґрунті расизму, расової дискримінації, ксенофобії і пов'язані з ними прояви нетерпимості, ненависті, насильства, усі форми жорстокого поводження з дітьми, включаючи педофілію й дитячу порнографію, а також торгівля людьми та їх експлуатація (ст. 59).

Більш розширені питання, які стосуються забезпечення ІПБ (інформаційно-психологічна безпека) у мережі Інтернет, регламентовані в регіональних актах Ради Європи. У першу чергу відзначимо «Декларацію про свободу обміну інформацією в Інтернеті» від 28 травня 2003 року [28], прийняту Комітетом міністрів Ради Європи. В основу документа закладена концепція балансу між свободою інформації в Інтернеті та інтересами інших осіб і держави. У ньому закріплені ряд принципів в області обміну інформацією в Інтернеті, які представляють інтерес у контексті проблеми ІПБ, до числа яких відносяться:

– контроль за змістом інформації в Інтернеті: держави не піддають зміст інформації в Інтернеті більшому обмеженню, ніж це стосується інших ЗМІ;

– регулювання або саморегулювання: держави повинні підтримувати регулювання або саморегулювання щодо змісту інформації, поширюваної в Інтернеті;

– відсутність державного контролю: суспільні органи влади не повинні забороннними або обмежувальними заходами перешкоджати доступу громадськості до інформації та вільному обміну інформацією в Інтернеті, незалежно від кордонів. Це не заважає встановити обмеження для захисту неповнолітніх користувачів, особливо в доступних місцях, таких як школи або бібліотеки. При дотриманні гарантій, передбачених п. 2 ст. 10 ЄКПЛ, можуть бути вжиті заходи, що зобов'язують видаляти чітко розпізнавану інформацію або блокувати доступ до неї в разі, якщо компетентні національні органи влади приймуть тимчасове або остаточне рішення про її незаконність;

– обмежена відповідальність служб надання інформації за зміст інформації в Інтернеті: держави не повинні накладати на служби надання інформації основні зобов'язання зі спостереження за змістом інформації в Інтернеті, до якої вони здійснюють доступ, передають або містять, а також за пошуком фактів чи обставин, що вказують на незаконну діяльність, так само як і відповідальність за зміст такої інформації;

– анонімність: для забезпечення захисту проти спостереження в мережі й розширення вільного обміну інформацією та думками держави повинні враховувати бажання користувачів Інтернетом не ідентифікувати свою особу. Це не заважає державам уживати заходів і співпрацювати для встановлення відповідальності за злочини, відповідно до національних законодавств, ЄКПЛ та інших міжнародних угод у галузі правосуддя та підтримки громадського порядку.

Питанням забезпечення безпеки неповнолітніх Інтернет-користувачів присвячені також інші нормативні документи Ради Європи у вигляді рекомендацій [29-31].

Що стосується Європейського Союзу, то ним були прийняті Рекомендації щодо захисту неповнолітніх та людської гід-

ності 98/560/ЄС від 24 вересня 1998 року та 2006/952/ЄС від 20 грудня 2006 року, які закріпили комплекс заходів, спрямованих на захист дітей від деструктивної інформації у ЗМІ та мережі «Інтернет», що реалізуються державами-членами ЄС, Європейською комісією, ЗМІ та іншими суб'єктами [32]. У документах наголошується зокрема, що держави-учасники повинні заохочувати пошук і впровадження нових способів захисту неповнолітніх й інформування користувачів; протидіяти поширенню в онлайн службах незаконного контенту, такого, що принижує людську гідність; сприяти забезпеченню безпечного використання аудіовізуальних та інформаційних онлайн послуг неповнолітніми; формувати відповідальну позицію з боку виробників, посередників і користувачів аудіовізуальних та інформаційних онлайн послуг; боротися з незаконною діяльністю в мережі Інтернет, яка може завдати шкоди неповнолітнім і т.ін.

Поряд із зазначеними правовими актами в Європейському Союзі діє Програма «Безпечний Інтернет» (Safer Internet Programme), мета якої полягає в розширенні прав і захисту дітей та молодих людей в онлайн шляхом реалізації ініціатив підвищення обізнаності та боротьби з незаконним і деструктивним контентом і поведінкою [33]. В основу Програми закладено багатосторонній підхід, спрямований на внесення вкладу в підвищення безпеки Інтернету всіма зацікавленими учасниками: національними правоохоронними органами, неурядовими організаціями, ученим співтовариством і органами корпоративного саморегулювання.

Для забезпечення підтримки та безпеки дітей в Інтернеті Програма «Безпечний Інтернет» передбачає реалізацію наступних напрямків діяльності:

– фінансування цільових проєктів, спрямованих на створення безпечного онлайн-середовища для дітей і підлітків;

– підтримку Дня безпечного Інтернету;

– організацію Форуму безпечного Інтернету;

– стимулювання й підтримку корпоративного саморегулювання;

– взаємодію з іншими міжнародними організаціями.

Програма ЄС «Безпечний Інтернет» реалізується переважно через цільові проєкти на національному та Європейському рівнях, спрямовані на створення безпечного онлайн-середовища для дітей і підлітків. Дані проєкти вирішують завдання підвищення обізнаності, боротьби з нелегальним контентом, фільтрації й маркування контенту, підтримку бази даних з інформацією про використання новітніх технологій молоддю, а також залучення громадянського суспільства в проблематику онлайн безпеки дітей.

Вельми цікавими прикладами участі громадянського суспільства у вирішенні завдання забезпечення безпеки дітей в Інтернеті в ЄС є Європейський молодіжний комітет (European Youth Panel) і Європейський батьківський комітет (European Parents Panel). Вони являють собою дискусійні майданчики, у форматі яких формулюються диференційовані думки дітей і дорослих із проблеми безпечного використання Інтернету, які в подальшому обговорюються в ширшому форматі на «Форумі безпечного Інтернету». Крім того, Центри безпечного Інтернету, що функціонують у країнах-членах ЄС, заснували національні молодіжні комітети, які консультують їх на регулярній основі.

4.3. Державне управління інформаційною безпекою дитини

Проблема інформаційної безпеки дітей, як уже було зазначено, є надзвичайно актуальною і зумовлює вирішення комплексу питань, пов'язаних із упорядкуванням інформаційного простору України, поглибленням наукових досліджень щодо протидії шкідливому впливу ЗМІ, удосконаленням нормативно-правової бази по відношенню до суб'єктів інформаційної діяльності. Рішення даної проблеми не можна досягти без ура-

хування гуманітарного чинника інформаційного середовища, оскільки «заборонні» функції держави сьогодні є малоефективними й нерідко стають об'єктом критики з боку інститутів громадянського суспільства. Необхідно також урахувати зарубіжний досвід щодо вирішення зазначених питань.

Б.А. Кормич підкреслює: «Компетенція держави у сфері інформаційної безпеки обумовлюється конкуренцією між інформаційними правами особи та функціями держави та її органів врегулювання інформаційних процесів та відносин. Тому в демократичному суспільстві державне регулювання інформаційної сфери має здійснюватися виключно шляхом установлення правових норм» [34]. На його думку, «інформаційна безпека людини та суспільства базується на нормах природного права і вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення», у той час, як інформаційна безпека держави «побудована на позитивному праві, пов'язана із застосуванням обмежень, заборон, жорсткою регламентацією, невід'ємним елементом яких є сила державного примусу».

Підтверджуючи позицію науковця, що при реалізації державної політики інформаційної безпеки на першому місці має бути метод переконання, зазначимо, що обмеження й заборони в сучасних умовах поступаються формуванню усвідомленого ставлення до норм правопорядку.

Організація ІБ дитини при одночасному дотриманні її прав і свобод, гарантованих національним та міжнародним правом, потребує ефективного функціонування в державі системи правових й організаційних заходів. Для створення ефективної системи протидії негативним інформаційним впливам на дітей та забезпечення їх ІБ потрібно чітко усвідомлювати загрози, механізми їхньої дії на свідомість дитини та наслідки, до яких може призвести їхня дія. Крім цього, у сучасних умовах України особливого значення, на думку Н.В. Ортинської, набувають правовідносини, що «виникають у разі військових конфліктів та екс-

тремальних ситуацій, які вимагають особливої ролі державних органів в охороні життя і здоров'я неповнолітніх» [5]. У проекції на інформаційну сферу можна відзначити проведення проти України масованих інформаційних операцій, спрямованих на деформацію свідомості її громадян, насамперед, тих, чия правосвідомість та система цінностей ще остаточно несформувалася. При забезпеченні ІБ неповнолітніх слід чітко диференціювати їхні категорії, обираючи особливий адміністративно-правовий інструментарій для дітей-сиріт, дітей-біженців, дітей, що опинилися в складних життєвих обставинах, із урахуванням норм міжнародного гуманітарного права.

Дитина як суб'єкт інформаційних відносин може взаємодіяти як у симплексному, так і в дуплексному режимах [35]. У першому випадку дитина отримує інформацію, не маючи зворотного зв'язку, а у другому – зворотно реагує і впливає на джерело інформації. Прикладом першого режиму є телебачення, коли дитина є пасивним отримувачем інформації. У другому випадку – це соціальні мережі, де дитина не лише отримує інформацію, але й має можливість реагувати на неї, створюючи та розповсюджуючи власний контент. В обох випадках взаємодії між суб'єктами інформаційних відносин характерним є відповідний розподіл соціальних функцій. Для телебачення притаманні інформаційно-пізнавальна та розважальна соціальна функція, а для соціальних мереж основною соціальною функцією є комунікаційно-інформаційна.

Розглядаючи інформаційні відносини з позиції форми взаємодії між суб'єктами можемо стверджувати, що кожному із них будуть притаманні певні ризики та загрози, а методи протидії їм носитимуть окремий характер і вимагатимуть різних організаційно-правових заходів.

При симплексному режимі інформаційної взаємодії відповідальність за забезпечення ІБ повинна нести держава. Має працювати чітка система регулювання та контролю з її боку за дотриманням законодавчо закріплених правових норм щодо

створення та обігу медійного контенту та запобігання поширення матеріалів, що можуть зашкодити психічному та фізичному здоров'ю дитини. Відповідальність за недотримання вимог чинного законодавства покладається на виробника та поширювача медійного продукту. Функції державних інститутів також полягають у контролі за дотриманням правових норм суб'єктами інформаційних відносин.

Зараз нормативно-правове регулювання у сфері ІБ дітей представлене переважно в контексті загальних прав і свобод дитини [15, 36] та в Законі України «Про основи національної безпеки України» [37]. Ці акти, декларативно торкаються зазначеної проблеми. Згідно зі статтею 52 Конституції України «Діти рівні у своїх правах, будь-яке насильство над дитиною та її експлуатація переслідуються за законом» [36]. Це положення деталізовано у п. 4 ст. 20 Закону України «Про охорону дитинства»: «Пропагування у ЗМІ культу насильства й жорстокості, розповсюдження порнографії та інформації, що зневажає людську гідність і завдає шкоди моральному благополуччю дитини, заборонено» [38]. Також серед положень вітчизняних законодавчих актів, що спрямовані на забезпечення ІБ дітей, є: ст. 5, 7 Закону України «Про захист суспільної моралі» [39], ст. 62 Закону України «Про телебачення й радіомовлення» [40], ст. 3 Закону України «Про друковані засоби масової інформації (пресу) в Україні» [41], ст. 20, п. 3 ст. 22 Закону України «Про рекламу» [42]. У вказаних правових актах можна виділити наступні нормативно закріплені принципи:

1) пріоритетність прав і законних інтересів дітей, особлива увага держави до їх захисту;

2) створення державою умов обігу інформаційної продукції, яка є безпечною для життя і здоров'я дітей та забезпечує їхній повноцінний розвиток і соціалізацію;

3) пріоритетність прав дитини на охорону моральності, здоров'я та забезпечення повноцінного розвитку перед інтересами забезпечення свободи слова та масової інформації, інши-

ми правами і свободами дорослих споживачів інформаційної продукції, а також її виробників і розповсюджувачів;

4) неприпустимість використання засобів масової інформації, інформаційно-телекомунікаційних мереж загального користування та інших засобів масової комунікації з метою пропаганди порнографії, насильства й жорстокості, наркотичних засобів і психотропних речовин, антигромадської поведінки;

5) повага до історичних і інших традицій і культурних цінностей держави і т.п.

У процесі вдосконалення сфери захисту дитини від шкідливої інформації слід враховувати вже існуючі на міжнародному рівні акти, а також досвід їхнього впровадження. Зокрема це стосується Модельного закону «Про захист дітей від інформації, що завдає шкоди їхньому здоров'ю та розвитку», прийнятого 3 грудня 2009 року на тридцять третьому пленарному засіданні Міжпарламентської Асамблеї держав-учасниць СНД [43], спрямованого на забезпечення дотримання обов'язків із забезпечення розробки належних принципів захисту дитини від інформації і матеріалів, що завдають шкоди її благополуччю», у тому числі від обороту дитячої порнографії, а також установлення необхідних обмежень прав самої дитини на свободу вираження поглядів, включаючи свободу шукати, одержувати, передавати інформацію та ідеї будь-якого роду. Закон дозволяє реалізувати в національному законодавстві держав-учасниць СНД гарантії захисту дитини від інформації, пропаганди та агітації, що завдають шкоди її здоров'ю, моральному та духовному розвитку.

У дуплексному режимі суб'єкти інформаційних відносин мають можливість здійснювати ряд дій з інформацією (створювати, передавати, приймати, трансформувати і т.ін.). У цьому випадку має бути застосована комплексна модель забезпечення ІБ дитини.

Закон України «Про основні засади розвитку інформаційного суспільства на 2007-2015 роки» визначає, що інформаційна безпека характеризується станом захищеності «важливих ін-

тересів людини, суспільства, держави, при якому запобігається завданняшкоди через негативний інформаційний вплив» [44]. Спираючись на змістовну частину щодо визначення національної безпеки в інформаційному просторі в Законі України «Про основи національної безпеки України» [37], можемо зробити висновок, що для забезпечення ІБ державі необхідно застосувати комплексну систему захисту у трьох основних напрямках:

– захист інформації, інформаційних ресурсів та забезпечення надійного функціонування інформаційно-комунікаційних систем, у тому числі систем критичної інфраструктури;

– забезпечення ефективної системи виявлення та протидії новітнім викликам і загрозам в інформаційному суспільстві, у тому числі й системі протидії негативним інформаційним та інформаційно-психологічним впливам на індивідуальну й колективну свідомість у суспільстві, недопущення впливу на неї через маніпулювання з інформацією;

– виховання в особи навичок та умінь із підвищення її інформаційної безпеки.

Очевидно, що зазначене повною мірою стосується дитини. Слід також відзначити те, що істотною вадою українського законодавства, на відміну від європейського, є відсутність реальних дієвих гарантій забезпечення охорони та захисту прав, свобод і законних інтересів дитини. Юридичні гарантії забезпечення, охорони та захисту прав дитини в Україні також потребують свого законодавчого закріплення, оскільки без них права дитини в багатьох випадках будуть залишатися лише декларацією.

Стратегія Ради Європи з прав дитини (2016 – 2021 рр.), про яку вже було сказано вище ([16]), спонукала Кабінет Міністрів України з метою імплементації європейських стандартів та підходів у забезпеченніправ дитини в Україні до видання 5 квітня 2017 року розпорядження № 230-р, яким було затверджено Концепцію Державної соціальної програми «Національний план

дій щодо реалізації Конвенції ООН про права дитини» на період до 2021 року [45].

У рамках даного документу серед інших основоположних принципів забезпечення правдитини передбачено й усебічний доступ до інформації і знань, необхідних для розвитку дитини з використанням досягнень сучасних інформаційно-комунікаційних технологій, відсутність дискримінації в інформаційній сфері, захист від усіх видів насильства, у тому числі й психологічного, а також створення безпечного інформаційного просторудля дітей, а саме:

– забезпечення захисту персональних даних дитини та іншої конфіденційної інформації про неї, забезпечення безпеки дітей в інформаційному просторі;

– формування політики запобігання проявам радикалізму, расизму, ксенофобії та іншим формам екстремізму в дітей в умовах стрімкого розвитку інформаційних технологій;

– унесення до освітніх програм для дітей віком від 7 до 14 років та програм підвищення кваліфікації вчителів питань безпеки дітей в інформаційному просторі;

– упровадження системи соціально-педагогічної роботи з батьками з питань безпеки дітей в інформаційному просторі.

Підсумовуючи викладене, можемо зазначити, що інтереси майбутнього країни та її безпеки постійно вимагають від органів державної влади України, регіонального керування, органів місцевого самоврядування, громадянського суспільства організації невідкладних заходів для поліпшення становища дітей та їх захисту. Останнє можливе при визначенні основних напрямків державної політики в інтересах дітей і ключових механізмів її реалізації, що базуються на загальновизнаних принципах і нормах міжнародного права [46].

Інструментом практичного вирішення багатьох питань у сфері інформаційної безпеки дитинства буде доцільна реалізація пріоритетних національних проєктів «Здорова дитина» та «Якісна освіта», цільових програм, прийняття низки найважли-

віших законодавчих актів, спрямованих на попередження найбільш серйозних загроз здійснення прав дітей, а саме: розробка Закону «Про інформаційну безпеку дітей», у якому буде чітке визначення понять «інформаційна безпека», «інформаційна грамотність», «інформаційний імунітет», «медіаграмотність». Даний Закон визначить правові основи радикального перетворення інформаційного простору українського суспільства з урахуванням потреби формування соціального середовища, сприятливого для повноцінного психічного й морально-духовного розвитку дітей.

4.4. Ювенальна юстиція в забезпеченні прав дитини

Ювенальна юстиція синтезує в собі два поняття, що походять із римського права: дитинство/молодість (від лат. Juvenalis – юний, молодий) і юстиція (від лат. Justitia – справедливість, правосуддя), і в найширшому розумінні означає справедливе ставлення до дітей і молоді. У сучасній юридичній науці поняття «ювенальна юстиція» єдиного й однозначного тлумачення не має.

Дослідники виділяють принаймні два підходи до визначення ювенальної юстиції та її системи, умовно називаючи їх широким і вузьким. Перший передбачає, що ювенальна юстиція – це система всіх ланок державного механізму, органів місцевого самоврядування, які займаються проблемами сім'ї та підлітків. Другий розглядає ювенальну юстицію в рамках судової системи як можливість створення спеціалізованих судових органів у справах сім'ї та неповнолітніх, удосконалення процесуальних форм при розгляді судом справ, що стосуються молоді [47].

За онтологічного статусу ювенальна юстиція може розглядатися як виключно державна система й діяльність або як інституція громадянського суспільства, що поєднує державні та недержавні органи та форми діяльності.

Державницька модель ювенальної юстиції передбачає наявність спеціалізованого суду, який здійснює правосуддя в справах неповнолітніх, усі інші інституції – державні та громадські – виконують допоміжні функції. Альтернативою судової моделі є адміністративна модель ювенальної юстиції, яка діє, зокрема, у Шотландії, де центральне місце займають адміністративні комісії у справах про правопорушення неповнолітніх. Позасудові способи вирішення конфліктів за участі дітей є в той же час і перевагою такої системи, і її недоліком, оскільки вони не здатні врегулювати конфлікти дитини з кримінальним законом.

У скандинавських країнах поєднуються судова й адміністративна ювенальна юстиція. Зокрема, у Швеції немає окремих ювенальних судів, але в місцевому суді працює ювенальний суддя або створюється ювенальний відділ суду для розгляду справ неповнолітніх. Провідну роль серед державних інститутів, що займаються захистом прав неповнолітніх у скандинавських країнах, грає соціальна служба, що організована за територіальним принципомі оперативно й ефективно вирішує проблеми конкретної дитини зусиллями фахівців, що працюють на території її проживання.

Цікавий досвід залучення до ювенальної юстиції інститутів громадянського суспільства має США, де існують недержавні підліткові суди, у яких дорослі або зовсім не беруть участі, або лише керують процедурою. У цих судах розглядаються справи про вперше вчинені неважкі злочини й проступки, якщо неповнолітній визнав свою провину. Примусові заходи, що застосовуються такими судами (відвідування спеціальних занять для подолання наркотичної або алкогольної залежності; грошова реституція, зобов'язання взяти участь у судовому засіданні підліткового суду як присяжний і т.п.), мають нерепресивний характер і значний виховний потенціал.

У багатьох державах, наприклад, у Нідерландах ефективно функціонують недержавні інститути виконання покарань для неповнолітніх правопорушників. У межах місцевої громади ви-

конується значна частина судових рішень у справах неповнолітніх, зокрема, громадські роботи (дрібний ремонт будівель, прибирання території і т.п.). У католицьких країнах (Іспанії, Італії, Португалії, Польщі) важливу роль у ювенальній юстиції відіграє церква.

Вітчизняні дослідники ювенальної юстиції пропонують «плюралістичну» модель, яка передбачає залучення до системи ювенальної юстиції поруч із державними органами інститути громадянського суспільства, поряд із правовими – медико-соціальні та психолого-педагогічні принципи (Н.М. Крестовська [48]). Концептуальне визначення ювенальної юстиції дається як «система державних, муніципальних і громадських судових, правоохоронних та правозахисних органів, установ і організацій, які на основі ювенального права і за допомогою медико-соціальних і психолого-педагогічних методів здійснюють правосуддя по відношенню до дітей, профілактику й попередження правопорушень дітей і проти дітей, захист прав, свобод та інтересів, а також ресоціалізацію дітей, які перебувають у складній життєвій ситуації».

Загальновизнаною метою системи ювенальної юстиції, яку задекларовано в усіх відповідних міжнародних положеннях щодо захисту прав людини, є реабілітація та соціальна реінтеграція дитини. Конвенція ООН про права дитини (ст. 40) проголошує: «Держави-сторони визнають право кожної дитини, яка, як вважається, порушила кримінальне законодавство, обвинувачується або визнається винною в його порушенні, на таке поводження, що сприяє розвиткові в дитини почуття гідності та значущості, зміцнює в ній повагу до прав людини й основних свобод інших та при якому беруться до уваги вік дитини й бажаність сприяння її реінтеграції та виконання нею корисної ролі в суспільстві» [15].

Відповідно до «Пекінських правил» [49], «система ювенальної юстиції спрямована, у першу чергу, на забезпечення благополуччя неповнолітнього й забезпечення того, щоб будь-

які заходи впливу на неповнолітніх правопорушників завжди були співвідносними як з особливостями особистості правопорушника, так і з обставинами правопорушення». Цей документ, на думку С. Закірової [50], виокремлює два головних і найважливіших завдання ювенальної юстиції. Перше завдання полягає в «забезпеченні благополуччя неповнолітнього», і, більше того, це головна з пріоритетних правових систем, де справи неповнолітніх розглядаються сімейними судами чи адміністративними органами», а й «тих судових систем, які дотримуються моделі кримінального переслідування», аби вони сприяли «уникненню застосування виключно каральних санкцій». Другим завданням є «принцип співвідносності», який розглядається, як «засіб для стримування важкості правопорушення», що в конкретному контексті означає, що «відповідь на дії молодих правопорушників має ґрунтуватися не тільки на ступені важкості правопорушення, а й з урахуванням особливостей особистості», таких, як «соціальний статус, ситуація в сім'ї, шкода, якої було завдано внаслідок правопорушення та інші чинники, які визначають особливості особистості».

Таким чином, за вимогами міжнародного законодавства про права людини, система ювенальної юстиції спрямована на сприяння реабілітації та соціальної реінтеграції дитини, включаючи формування в дитини відчуття гідності та цінності її особистості, а також виховання поваги до фундаментальних прав інших людей.

Із іншого боку, мета ювенальної юстиції представляється також як триєдиний комплекс: 1) відновлення прав і "зцілення" жертви; 2) визнання правопорушником заподіяної ним шкоди і прийняття на себе відповідальності за усунення цієї шкоди; 3) досягнення примирення між жертвою, правопорушником і співтовариством, у якому вони живуть [3].

Ефективним засобом досягнення зазначеної мети є медіація, яка сьогодні впроваджена в систему ювенальної юстиції багатьох країн світу. Медіація – це процес добровільного, зрілo-

го й усвідомленого вирішення спору проактивними сторонами на підставі принципів взаємної поваги, рівності і «виграють всі» («win-win») за посередництва нейтральної, незалежної й неупередженої, але компетентної особи – медіатора, який допомагає сторонам прийти до взаємоприйнятного рішення [51]. У порівнянні з іншими способами вирішення спору (судового чи арбітражного/третейського) сторони самі контролюють процес медіації та його результати, а медіатор не виносить обов'язкового для сторін рішення й не зобов'язує сторони підписувати медитативні угоди й дотримуватися їх. У разі успіху медіації сторони підписують медіативну угоду й добровільно виконують її, в іншому випадку – ідуть до суду.

За приклад можна навести досвід країн, де медіація використовується для вирішення спорів на рівні із судовими процесами та закріплена конкретними нормативно-правовими актами.

Говорячи про законодавче регулювання медіації у Сполучених Штатах Америки, зазначимо, що вже у 1981 р. Каліфорнія стала першим штатом, у якому медіація була запропонована для вирішення суперечок, пов'язаних з опікою над дітьми. Для американців є дуже важливим нерозголошення конфіденційної інформації. У США більше 250 правил конфіденційності та привілеїв, що діють у різних штатах, визначають питання про те, яка саме інформація може бути розкрита в процесі медіації без побоювання її подальшого поширення. Із цією метою був розроблений Однаковий закон про медіацію (The Uniform Mediation Act) [52].

Що стосується європейської практики запровадження медіації, «Директива 2008/52/ЄС Європейського Парламенту та Ради з певних аспектів медіації в цивільних і комерційних справах», затверджена в 2008 р., передбачає імплементацію норм у законодавство держав-членів. Зазначена Директива закріплює основні принципи проведення та запровадження процедури медіації в національне законодавство країн-членів ЄС [53].

Правові основи взаємодії сім'ї і системи ювенальної юстиції закладені в міжнародних стандартах ювенальної юстиції: відповідних положеннях Конвенції ООН про права дитини (1989) [15], Пекінських правилах (1985) [49], Ер-Ріядських керівних принципах (1990) [54], Гаванських правилах (1990) [55], Європейських правилах (2008) [56] та ін.

Базовими положеннями зазначених імперативних і рекомендаційних актів щодо забезпечення взаємодії сім'ї і системи ювенальної юстиції є:

– вимога негайного інформування батьків про всі процедури й можливі санкції щодо неповнолітнього;

– забезпечення участі батьків на всіх стадіях слідства у справі неповнолітнього;

– вимога збереження сімейного середовища неповнолітнього правопорушника.

Відзначимо, що норми та практика зарубіжних систем ювенальної юстиції містять багато напрацювань щодо залучення сім'ї до виконання основної функції ювенального правосуддя – соціальної реінтеграції неповнолітнього правопорушника. Особливо це стосується первинної і вторинної профілактики правопорушень неповнолітніх. Імовірність протиправної поведінки можна зменшити шляхом зміцнення соціальних зв'язків неповнолітнього з сім'єю, школою та іншими інститутами громадянського суспільства. Що стосується третинної профілактики, то сімейна й подібна до неї атмосфера створює найкращі умови для перевиховання таресоціалізації неповнолітнього правопорушника.

Найвідоміша практика – сімейні конференції (СК) у системі ювенальної юстиції Нової Зеландії. У СК беруть участь неповнолітній правопорушник, члени його сім'ї, жертва й особи, які її підтримують, адвокат у справах молоді (на вимогу підлітка), соціальний працівник (тільки в певних випадках) і будь-які інші особи, за бажанням сім'ї, досвід яких може виявитися корисним для підлітка. У ході СК проходить широке обговорення того,

що сталося і вирішується, чи слід переслідувати підлітка в кримінальному порядку, і якщо ні, то яким чином вирішити справу, причому пріоритет віддається альтернативним (некаральним) заходам. СК виробляє план дій, наприклад, правопорушник приносить свої вибачення жертві, відшкодовує збиток (у грошовому еквіваленті або у вигляді роботи в інтересах жертви), виконує громадську роботу тощо.

У цьому випадку судові слухання відкладаються до закінчення виконання плану. Якщо консенсусу не досягнуто, справа знову передається в суд або поліцію (залежно від того, від кого вона потрапила на СК).

Що стосується України, то перелічені вище базові положення ювенальної юстиції лише частково відображені в чинному законодавстві, хоча сім'я неповнолітнього правопорушника є активним агентом ювенальних практик. Так, чинним кримінальним законодавством України передбачені такі види примусових заходів виховного характеру, як обмеження дозвілля і встановлення особливих вимог щодо поведінки неповнолітнього (п. 2 ч. 2 ст. 105 Кримінального кодексу), передача неповнолітнього під нагляд батьків або осіб, які їх заміняють (п. 3 ч. 2 ст. 105 Кримінального кодексу). В обох випадках передбачається активна участь батьків у реалізації виховної функції ювенальної юстиції. Інша справа, що батьки потребують допомоги у виконанні цих видів заходів. Їх потрібно, по-перше, навчити, як прищепити дитині навички правослухняної відповідальної поведінки; по-друге, навчити співпрацювати з системою ювенальної юстиції, а не протистояти їй; по-третє, зобов'язати виконувати законні приписи й розпорядження суб'єктів ювенальної юстиції.

Не можна не погодитися з думкою [57], що в майбутньому законі України, що стосується ювенальної юстиції, повинен бути окремий розділ, присвячений родині як її складовій, де повинні бути відображені такі правоположения:

1. Батьки й інші законні представники дитини повинні виховувати дитину в дусі законослухняності, поваги до моральних цінностей, прав і свобод інших людей.

2. Батьки або інші законні представники дитини в разі його конфлікту з законом мають право бути присутніми на всіх стадіях ведення справи про правопорушення неповнолітнього.

3. Батьки або інші законні представники дитини в разі його конфлікту з законом дають згоду на напрям дитини на примирливу або корекційну програму. Відмова не береться до уваги, якщо він суперечить інтересам дитини.

4. Дитина з девіантною поведінкою може бути спрямована на корекційну програму службою у справах дітей за ініціативою батьків або інших законних представників дитини.

5. Батьки або інші законні представники дитини в разі її конфлікту з законом зобов'язані сприяти ресоціалізації їхньої дитини шляхом виконання законних вимог суб'єкта ювенальної юстиції, співпраці з навчальним закладом, установою освіти, трудовим колективом, громадськими та благодійними організаціями, які залучені до справи ресоціалізації їхньої дитини.

6. Батьки або інші законні представники дитини в разі її конфлікту з законом зобов'язані сприяти виконанню примирної або корекційної програми, на яку неповнолітній підозрюваний або звинувачений був направлений суб'єктом ювенальної юстиції.

7. У разі ухилення без поважних причин від зобов'язань, покладених на батьків або інших законних представників дитини в разі її конфлікту з законом, вони несуть відповідальність відповідно до законодавства.

Розвиток адміністративно-правового регулювання прав дитини в Україні важливий насамперед тому, що, як підкреслює Н.М. Крестовська (і з цим важко сперечатись), «…охорона дитинства та захист прав дітей об'єктивно стають одним із пріоритетів юридичного забезпечення національної безпеки, оскільки наявна депопуляція та невтішні демографічні прогнози, рівень

якості життя дітей та молоді, що не відповідає гуманітарним світовим стандартам, зниження освіченості, незадовільний стан правової культури, відсутність позитивної динаміки у протидії негативним явищам у дитячому та молодіжному середовищі ставлять під загрозу майбутнє та саме існування українського суспільства» [48].

В Україні діє розгалужена система захисту прав дітей, але діти, які скоїли протиправне діяння, зазвичай потрапляють під юрисдикцію органів кримінального правосуддя. Проблема адекватної реакції держави та суспільства на ситуацію із правопорушеннями серед дітей і молоді особливо гостро постала в роки незалежності. На даний час не припиняються спроби впровадити більш гуманну систему роботи з дітьми, які з законом у конфлікті.

Н.М. Крестовська пропонує запровадити поняття «ювенальна відповідальність», яке застосовується до дитини-правопорушника. На її думку, даний вид відповідальності застосовується і виконується не тільки державними органами, але й іншими соціальними суб'єктами, якими є недержавні органи та служби у справах дітей, медіатори, громадські організації, адміністрація навчальних закладів, недержавні суди, недержавні виховні установи тощо.

О.О. Навроцький, говорячи про специфіку національної моделі законодавчої регламентації прав дитини, наголошує на відсутності в системі законодавства України уніфікованого нормативного акта, регуляторний потенціал якого всебічно був би спрямований на забезпечення прав, свобод ізаконних інтересів дитини [58]. Визначаючи поняття «адміністративно-правові гарантії забезпечення прав дитини», науковець пропонує їх диференціацію на нормативні, організаційні та безпекові гарантії.

В Україні існують деякі правові та організаційні передумови для формування системи ювенальної юстиції, однак її судовий елемент залишається найбільшою проблемою, яка потребує вирішення на законодавчому рівні. Окремі кроки в

цьому напрямку вже зроблені. Указом Президента України від 10.05.2006 №361/2006 було схвалено «Концепцію вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів» [59]. Згідно з Концепцією, на одному з етапів реформи системи судів загальної юрисдикції необхідно впровадити спеціалізацію судів з поділом на цивільні, кримінальні та адміністративні, передбачивши в них спеціалізацію суддів, у тому числі за суб'єктною ознакою (наприклад, у справах неповнолітніх). Концепція вказує на необхідність запозичення позитивного досвіду демократичних держав із реституційного правосуддя, яке полягає не в покаранні особи, а в примиренні обвинуваченого та потерпілого за участі посередника (медіатора) і/або у відшкодуванні потерпілому завданої матеріальної та моральної шкоди.

Указом Президента України № 597/2011 від 24.05.2011 схвалено «Концепцію розвитку кримінальної юстиції щодо неповнолітніх в Україні», де визначено, необхідність побудови в Україні повноцінної системи кримінальної юстиції, здатної забезпечити законність, обґрунтованість та ефективність кожного рішення щодо дитини, яка потрапила в конфлікт із законом, пов'язаного з її перевихованням та подальшою соціальною підтримкою [60].

Ще одним кроком до ювенальної юстиції в Україні стало доповнення до ст. 18 Закону України «Про Судоустрій і статус суддів», згідно з яким,«У місцевих загальних судах та апеляційних судах діє спеціалізація суддів із здійснення кримінального провадження щодо неповнолітніх» [61].

Важливе значення має впровадження інституції Уповноваженого з прав дитини при Президентові України, мета якої – забезпечення належних умов для реалізації громадянських, економічних, соціальних та культурних прав дітей в Україні, беручи до уваги необхідність особливого піклування про дитину, на виконання Україною міжнародних зобов'язань у сфері прав дитини [62].

Ще 2013 року у Верховній Раді України був зареєстрований законопроєкт № 2425а-1 «Про медіацію», у якому передбачено й участь дитини в процедурі медіації, однак у 2014 році законопроєкт був відкликаний.

У 2014 р. Україна підписала Угоду про Асоціацію з Європейським Союзом. Згідно зі ст. 1 Угоди, Україна і ЄС мають посилювати співпрацю у сфері юстиції, свободи та безпеки з метою забезпечення верховенства права та поваги до прав людини та основоположних свобод [63]. Країни Європейського Союзу погодилися, що забезпечення верховенства права та кращого доступу до правосуддя повинно включати доступ як до судових, так і до позасудових методів врегулювання спорів.

Пізніше Указом Президента України №276/2015 від 20.05.2015 р. була схвалена «Стратегія реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 рр.». Відповідно до п. 5.4. Стратегії, передбачено розширення способів альтернативного (позасудового) врегулювання спорів (зокрема, шляхом практичного впровадження інституту медіації та посередництва) [64].

Зараз у Верховній Раді України новий проєкт Закону «Про медіацію» (№3665) пройшов перше читання й наразі триває його доопрацювання до другого читання. У Статті 2 (Сфера застосування медіації), п.5. указано, що «Медіація застосовується під час вирішення сімейних спорів (конфліктів), якщо такі спори (конфлікти) впливають чи можуть вплинути на права й законні інтереси дитини, зокрема як третьої особи, відповідно до законодавства та з урахуванням найкращих інтересів дитини» [65].

Після прийняття закону єдиною перешкодою для стрімкого розвитку медіації в Україні може стати низький рівень знань про медіацію серед звичайних громадян, що може породжувати недовіру до такої процедури. Проте медіація в Україні є цілком реальною, але потрібно пройти шлях визначення цієї процедури на законодавчому рівні.

Незважаючи на, здавалося б, очевидність необхідності розвитку ювенальної юстиції, в Україні багато її противників. Існує думка, що ювенальна юстиція узаконює неповагу дітей до батьків і не дозволить застосувати до дитини примус, без якого виховання неможливо. Н. Крестовська вважає, що наші громадяни просто плутають примус, насильство й покарання, повністю ототожнюючи їх [66]. Насправді, жоден із нормативно-правових актів із питань ювенальної юстиції не ставить під сумнів необхідність поєднання переконання і примусу в процесі виховання дитини. Забороняється батьківське насильство (його визначення є в Законі України «Про попередження насильства в сім'ї» [67]), виконання покарання покладається на державні органи, а примус (зрозуміло, що без побиття) як був, так і залишається одним із методів виховання.

Серед інших аргументів противників ювенальної юстиції звучить такий, що в Україні і так достатньо інститутів, що займаються проблемами дітей. Частково погоджуючись із тим, що ювенальна юстиція, хоча й незавершена і недосконала, в Україні вже існує і відображена в багатьох законодавчих актах, актуальним є приведення цієї системи у відповідність до потреб підростаючого покоління і всього українського суспільства й до міжнародних зобов'язань держави у сфері захисту прав дитини. Реформування ювенальної юстиції в Україні – це лише питання часу, і хотілося б, щоб він не витрачався даремно.

Підсумовуючи, маємо зазначити, що наразі функціонує Міжвідомча координаційна рада з питань правосуддя щодо неповнолітніх – консультативно-дорадчий орган КМУ, утворений згідно з постановою КМУ від 24 травня 2017 року №357 з метою запровадження міжінституційної платформи для системного обговорення та вирішення проблемних питань розвитку правосуддя щодо неповнолітніх, прийняття узгоджених рішень, що відповідають інтересам дитини.

Ключовими завданнями Міжвідомчої координаційної ради є:

– координація дій органів виконавчої влади з метою забезпечення розвитку політик і практик забезпечення інтересів неповнолітніх, які вчинили кримінальне правопорушення, стали жертвами або свідками злочинів;

– дослідження спроможності запуску єдиної системи органів, що працюють із дітьми;

– удосконалення нормативно-правової бази з питань правосуддя щодо неповнолітніх із урахуванням досвіду зарубіжного законодавця;

– формування достатніх пропозицій запровадження ефективного правосуддя щодо неповнолітніх, які вчинили правопорушення;

– вивчення шляхів вирішення проблемних питань функціонування відновного правосуддя в Україні.

Серед конкретних планів Міжвідомчої координаційної ради є:

– вивчення необхідності розробки законопроєкту про внесення змін до Закону України «Про безоплатну правову допомогу» щодо надання безоплатної первинної та вторинної правової допомоги дитині та інформування її про свої права і свободи, порядок їхньої реалізації;

– розробка проєкту Закону України «Про ювенальну юстицію» з урахуванням міжнародних стандартів забезпечення розбудови системи ювенальної юстиції;

– затвердження Стратегії попередження злочинності неповнолітніх [68].

На сучасному етапі суспільного розвитку вплив інформації на дитину актуалізується не тільки в плані психолого-педагогічної проблеми, але й у правовій площині. Інформаційна безпека дитини розглядається як сегмент інформаційної безпеки суспільства й держави, а тому потрапляє у правові відносини, що мають регулюватися державою.

Як було зазначено раніше [69], сукупність явищ і проблем, пов'язаних із глобальною інформатизацією, призвели до появи

інформаційного права – комплексного поєднання науки й галузі права, яке відокремилось від інших суспільних відносин у самостійний вид на підставі історичного розвитку людської формації, розвитку новітніх технологій, які потребують якісно нових способів і прийомів регулювання інформаційних відносин.

Погоджуючись із О.А. Барановим [70], який пропонує в якості базового принципу інформаційного права використовувати принцип забезпечення інформаційної безпеки, зазначимо, що забезпечення ІБ є однією з основних атрибутивних особливостей систем, у тому числі соціальних. Цей принцип знайшов відображення й у ст.17 Конституції України, про що вже наголошувалось раніше. Похідними від цього принципу в даному контексті виділимо наступні:

– свобода отримання й поширення інформації;

– об'єктивність, достовірність, повнота й точність інформації;

– гармонізація інтересів особистості, суспільства й держави в інформаційній діяльності;

– мінімізація негативного інформаційного впливу;

– об'єктивність надання інформації;

– обмеження доступу до інформації;

– гармонізація українського законодавства щодо регулювання інформаційних відносин із міжнародним законодавством.

Підставою для виділення ІБД у якості об’єкта правового регулювання, на думку Топчій О.В. [4], є значущість для держави й суспільства захисту інформаційних прав та інтересів дитини на тлі забезпечення її безпеки. З іншого боку, не менш важливим є й те, що ІБД виступає як складова інформаційної безпеки особи, суспільства й держави. У разі реалізації загроз і ризиків в одній зі складових виникає збій у життєдіяльності всієї системи.

В Україні наразі відсутнє консолідоване законодавство щодо забезпечення прав, свобод і законних інтересів дитини, про що було наголошено раніше, тим більше, неврегульовані інформаційні правовідносини щодо захисту й забезпечення

законних інтересів дітей в інформаційній сфері. Норми права в досліджуваному ракурсі розкидані в сотнях нормативно-правових актів і в абсолютній більшості зорієнтовані на дорослих суб'єктів, а не на дитину. Ті законодавчі акти, що розглядалися впродовж розділу, спрямовані насамперед на забезпечення інформаційної безпеки держави в цілому. Про забезпечення ІБД у них взагалі не йдеться. Крім цього, творці правових норм зосереджуються в основному лише на необхідності захисту дитини від негативного впливу інформації. Майже не враховується те, що поняття інформаційної безпеки особи має більш широке трактування. Топчій О.В. пропонує власну концепцію класифікації видів ІБД, яка, на її думку, може полегшити дослідження інформаційної безпеки неповнолітніх та втілення основних засад у державну інформаційну політику, нормативно-правові акти, практику правозастосування. Вона виділяє: інформаційно-психологічну, інформаційно-валеологічну, інформаційно-соціальну, інформаційно-правову, інформаційно-економічну та інформаційно-технічну безпеку. Наведемо коротку характеристику кожного із зазначених видів.

Інформаційно-психологічна безпека – стан, процес і результат цілеспрямованої діяльності держави, інститутів громадянського суспільства, усіх свідомих суб'єктів інформаційних правовідносин щодо захисту психіки і свідомості особи від деструктивних впливів, створення умов для повноцінного гармонійного розвитку та самореалізації особистості.

Головним інструментарієм забезпечення ІПБ дитини виступає експертна, консультативна, просвітницька, корекційна діяльність психологів і педагогів, їхні рекомендації уповноваженим органам влади щодо нормативного врегулювання процесів розповсюдження не бажаної для суспільства інформації.

Інформаційно-валеологічна безпека – вид інформаційної безпеки, спрямований на захист особи від негативного впливу інформації, яка може призвести до суїциду або особливо небезпечних травм чи хвороб, погіршення стану здоров'я через

куріння, вживання алкогольних, наркотичних та ін. шкідливих речовин, нерозбірливих статевих відносин, навмисного пошкодження частин тілу чи шкіри (у тому числі через шрамінг або татуювання), потягу до нездорової їжі (фастфуду) чи біодобавок, із одночасним протиставленням цьому здорового способу життя, культури тіла й фізичної активності.

Головним інструментарієм забезпечення інформаційно-валеологічної безпеки дитини виступає праворегулювальна й правозастосовна діяльність, зокрема в частині нормування змісту кіно-, теле- і медіапродукції, реклами; адміністрування просвітницької та дозвільної роботи шкільних і позашкільних закладів освіти; діяльність органів місцевого самоврядування щодо стану довкілля, упорядкування територій, організації спортивних майданчиків; своєчасна реакція на появу так званих наркографіті з інформацією щодо джерел придбання шкідливих для здоров'я речовин; створення завдяки адміністративним засобам відповідального батьківства.

Інформаційно-правова безпека – невід'ємна частина інформаційної безпеки, спрямована на застосування правових механізмів для захисту інформаційних прав і свобод, безперешкодної реалізації громадянської освіти, убезпечення дитини від не призначеної для неї інформації та упередження інформаційних деліктів.

Зазначений вид безпеки тісно пов'язаний із такими юридичними категоріями, як «правова культура», «правове виховання», «правова просвіта», «правова свідомість», «безпечне інформаційне середовище» тощо. Даний вид інформаційної безпеки складається з норм із захисту й дотримання інформаційних прав неповнолітнього і норм щодо превенції інформаційних правопорушень.

Інформаційно-соціальна безпека – сегмент безпеки, за якого правовими, організаційно-управлінськими та ін. засобами створюються умови для повноцінного розвитку особистості як достойного законослухняного члена суспільства з активною

громадянською позицією й убезпечення неповнолітньої особи від негативних інформаційних впливів деструктивних спільнот (кримінальних, екстремістських, релігійних та ін.).

Інструментарієм забезпечення інформаційно-соціальної безпеки виступає не тільки правове регулювання інформаційних правовідносин, а й важелі державної інформаційної політики, адміністративне сприяння підтримці соціально-етичних норм, скерування освітньо-виховних засобів тощо.

Інформаційно-економічна безпека – складова інформаційної безпеки, яка передбачає убезпечення дитини та її родини від нанесення матеріальної шкоди як окремій особі, так і її родині внаслідок агресивної реклами інтернет-шопінгу, нав'язування сумнівних послуг, залучення до азартних ігор (у тому числі інтернет-казіно), участі в сумнівних фінансових проєктах. Відтак виникає необхідність запровадження в системі освіти елементів фінансової грамотності із роз'ясненням сутності та наслідків матеріальних ризиків, включенням до стандартів медіаосвіти тем, пов'язаних із маніпулюванням свідомістю не тільки в політичній сфері, а й у торговельно-фінансових відносинах на рівні бюджету сім'ї.

Інформаційно-технічна безпека – складова, що передбачає поєднання інформаційно-технологічних компетенцій із застосуванням заходів технічної безпеки, формуванням відповідального ставлення до роботи з інформацією, ресурсами, пристроями, до процедур збирання, зберігання, поширення інформації. Даний вид інформаційної безпеки тісно взаємопов'язаний із кібербезпекою, оскільки реалізується у безпосередньому спілкуванні із застосуванням відповідних технічних засобів.

Інструментарієм забезпечення інформаційно-технічної безпеки є, насамперед, комплекс технічних заходів, використання спеціального програмного забезпечення, у тому числі систем батьківського контролю в поєднанні із освітньо-виховною діяльністю.

Правове регулювання інформаційної сфери дитини повинно охоплювати весь спектр розглянутих видів ІБД. Від укладачів закону потребується пошук балансу між співвідношенням державних, суспільних інтересів та інформаційних інтересів особистості, що базуються на правах людини. Мусимо констатувати, що наразі ключовий термін «Інформаційна безпека дитини» ще залишається в лоні доктринальних підходів у праві й не знаходить свого відображення в законодавстві, хоча формальний склад закріплених в існуючих нормативно-правових актах кореспондується із поняттям ІБД. Законодавство потребує суттєвої модернізації, приведення у відповідність до реалій сьогодення.

На думку Топчій О.В., вагомим теоретичним джерелом формування концепції ІБД є безпекознавство – суспільна міждисциплінарна наука, яка досліджує загальні та специфічні об'єктивні закономірності організації та функціонування систем безпеки різного класу і виробляє на підставі їх пізнання загальні теоретичні положення, які спрямовані на підвищення ефективності їх функціонування (Ліпкан В.А. [71]). Топчій О.В. пропонує в розділі інформаційного безпекознавства створити *інформаційно-ювенальне безпекознавство* як підгалузь, «що має на меті дослідження і впровадження у практичну діяльність концептуального конгломерату адміністративно-правових, організаційно-управлінських, науково-технічних, психолого-педагогічних засад пізнання та діагностики інформаційних загроз та ризиків негативного впливу на неповнолітнього, забезпечення взаємодії органів державної влади та інституцій громадянського суспільства в контексті публічного управління задля одночасного підтримання безпечного інформаційного середовища і формування інформаційного імунітету особистості, вибору ефективних засобів превенції та протидії інформаційним деліктам» [4].

У якості складових елементів запропонованої підгалузі пропонується розглядати *інформаційно-ювенальну превентологію* (як напрям, що досліджує профілактику/попередження

правопорушень у сфері інформаційної безпеки неповнолітніх, запобігання негативним інформаційним впливам на особистість на етапі її соціалізації), *інформаційно-ювенальну деліктологію* (як напрям, що досліджує правопорушення неповнолітніми інформаційної безпеки інших осіб або комп'ютерних систем або посягання дієздатних осіб на ІБД), ювенальну *інформаційно-безпекову компаративістику* (як напрям порівняльного правознавства, у межах якого досліджуються міжнародно-правові акти та нормативні акти інших держав, закордонний практичний досвід забезпечення ІБД, шляхи адаптації цих знань до української дійсності).

У цілому погоджуючись з ідеями автора, зазначимо що інтеграція наукових засад адміністративного й інформаційного права, інформаційного безпекознавства із ювенальним правом має перспективу створення міцного теоретичного підґрунтя для практичного забезпечення інформаційної безпеки дітей, що може сприяти консолідації українського суспільства на сучасному етапі.

Список використаних джерел

1. Фурашев В.М. Державно-правові проблеми інформаційної безпеки людини і суспільства в умовах інтеграції України у світовий інформаційний простір. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали наук.-практ. конф. 06 жовт. 2016 р. Упоряд.: В. М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського». Вид-во «Політехніка». 2016. С. 7-24.

2. Радзієвська О.Г. Проблеми негативних інформаційних впливів на дитину в Україні в умовах збройного протистояння. Науковий вісник Ужгородського національного університету. Серія ПРАВО. Випуск 42. 2017. С.197-200.

3. Панченко О.А. Информационная безопасность ребенка: Монография. Киев: КВИЦ. 2016. 380 с.

4. Топчій О.В. Адміністративно-правове забезпечення інформаційної безпеки неповнолітніх в Україні: дис. д-ра юрид. наук: 12.00.07. Державний вищий навчальний заклад «Ужгородський національний університет». Ужгород. 2019. 479 с. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/20163 (дата звернення: 14.04.2020).

5. Ортинська Н.В. Правовий статус неповнолітніх: теоретико-правове дослідження : дис. … д-ра юрид. наук : 12.00.01. Національний університет «Львівська політехніка». Львів. 2017. 453 с.

6. Радзієвська О.Г. Дитина у глобалізованому інформаційному просторі: реальні та потенційні загрози. Інформація і право. № 4 (19). 2016. С. 29-38.

7. Брайант Д., Томпсон С. Основы воздействия СМИ. М.: Издательский дом «Вильямс». 2004. 424 с.

8. Медиа-насилие: детям прививают страсть к убийству. Интервью с полковником Дэвидом Гроссманом. URL: http://www.pravoslavie.ru /jurnal/783.htm (дата звернення: 10.04.2020).

9. Соціологія: підручник / за ред. В. Г. Городяненка. 3-тє вид., переробл. і доп. К.: ВЦ «Академія». 2008. 544 с.

10. Вплив соціальних мереж на формування особистості підлітків. Науковий звіт. URL:https://vipsoft.blob.core.windows.net/contest/041cf057f5dfb5204385e35b82eed715.pdf (дата звернення: 10.04.2020).

11. Социальные сети. Как защитить ребенка. URL: https://shcherbakovs.com/how-to-protect-kids-in-social-media/ (дата звернення: 10.07.2020).

12. Teens, SocialMedia&Technology 2018. URL: https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/ (дата звернення: 10.04.2020).

13. ScialMediaStatistics. URL: https://www.guardchild.com/social-media-statistics-2/ (дата звернення: 10.04.2020).

14. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217

A (III) от 10 декабря 1948 г.).URL: http://zakon3.rada.gov.ua/laws/show/995_015 (дата звернення: 10.04.2020).

15. Конвенция о правах ребенка (Нью-Йорк, 20 ноября 1989 г.). URL: https://www.icrc.org/rus/resources/documents/misc/treaties-children-convention-201189.htm (дата звернення: 10.04.2020).

16.Council of Europe Strategy for the right sof the child 2016. 2021 : Council of Europe; Strasbourg, 6 November 2015. URL: https://rm.coe.int/168048dee3 (дата звернення: 10.04.2020).

17. Международный пакт о гражданских и политических правах (принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года). URL:http://zakon2.rada.gov.ua/laws/show/995_043. (дата звернення: 10.04.2020).

18. Декларация об основных принципах, касающихся вклада средств массовой информации в укрепление мира и международного взаимопонимания, в развитие прав человека и в борьбу против расизма и апартеида и подстрекательства к войне от 28 ноября 1978 года. URL: http://zakon4.rada.gov.ua/laws/show/995_393.(дата звернення: 10.04.2020).

19. Конвенция о защите прав человека и основных свобод (г. Рим, 4.XI.1950 г). URL: http://www.irs.in.ua/index.php?option=com_ (дата звернення: 10.04.2020).

20. Резолюция N 428 (1970) Консультативной ассамблеи Совета Европы «Относительно Декларации о средствах массовой информации и правах человека» (23 января 1970 года). URL: http://zakon1.rada.gov.ua/laws/show/994_107 (дата звернення: 10.04.2020).

21. Декларация о свободе выражения мнения и информации (Принята Комитетом министров Совета Европы, 29 апреля 1982г.). URL:/ http:/cyberpeace.org.ua/files/ii_a_3.pdf (дата звернення: 10.04.2020).

22. Конвенция о трансграничном телевидении от 5 мая 1989 г. URL: http://zakon4.rada.gov.ua/laws/show/994_444 (дата звернення: 10.04.2020).

23. Договор о Европейском Союзе. Европейский Союз: Основополагающие акты в редакции Лиссабонского договора с комментариями. Отв. ред. С.Ю. Кашкин. М.: ИНФРА-М. 2010. С. 166-210.

24. Директива Совета Европейского Союза 89/552/ЕЕС о координации определенных положений, установленных законодательно, регулятивно либо административно странами-участниками (Европейской Конвенции о трансграничном телевещании) в области осуществления телевизионного вещания (в редакции Директивы 97/36/ЕС Европейского Парламента и Совета от 19 июня 1997 года). URL: http://zakon4.rada.gov.ua/laws/show/994_446 (дата звернення: 10.07.2020).

25. Директива Європейського Парламенту та Ради Європи 2010/13/ЄС від 10 березня 2010 року про узгодження певних положень, визначених законами, підзаконними актами та адміністративними положеннями у державах-членах стосовно надання аудіовізуальних медіапослуг (Директива про аудіовізуальні медіапослуги) (кодифікована верія). URL:http://medialaw.org.ua/library/dyrektyva-yevropejskogo-parlamentu-ta-rady-yevropy-2010-13-yes/ (дата звернення: 10.04.2020).

26. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 года). URL: http://zakon2.rada.gov.ua/laws/show/998_163 (дата звернення: 10.04.2020).

27. Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (12 декабря 2003 года). URL: http://zakon4.rada.gov.ua/laws/show/995_c57 (дата звернення: 10.04.2020).

28. Декларация о свободе обмена информацией в Интернете. URL: http://docs.pravo.ru/document/view/17327961/14974117 (дата звернення: 10.04.2020).

29. Рекомендация № r (2001) 8* Комитета министров Совета Европы государствам-членам «О вопросах саморегулирования виртуального содержания (саморегулирование и охрана пользователей от противоправного или причиняющего

вред содержания новых информационных и коммуникационных услуг)» (Принята Комитетом Министров 5 сентября 2001 г. на 762-ом заседании Представителей Министров. URL: http://echr-base.ru/rec2001_8.jsp (дата звернення: 10.04.2020).

30. Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment.URL: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2009)5&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75). (дата звернення: 10.04.2020).

31. Рекомендация Парламентской Ассамблеи Совета Европы № 1882 (2009) от 28 сентября 2009 г. «Продвижение Интернет- и онлайновых ресурсов, безопасных для несовершеннолетних». URL: http://www.coe.int/T/r/Parliamentary_Assembly/%5BRussian_documents%5D/%5B2009%5D/%5BSepOct2009%5D/Rec1882_rus.asp (дата звернення: 10.04.2020).

32. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Монография. М.: НИТИ-ДАНА. 2011. URL:http://spkurdyumov.ru/uploads//2013/08/smirnov.pdf. (дата звернення: 10.04.2020).

33. Safer Internet Programme: Empowering and Protecting Children online.url: http://ec.europa.eu/information_society/activities/sip/index_en.htm. (дата звернення: 10.04.2020).

34. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України. Дис. … д-ра юрид. наук: 12.00.07. Одеська національна юридична академія. Одеса. 2004. 427 с.

35. Радзієвська О.Г. Правові засади та пріоритети розвитку протидії негативним інформаційним впливам на дітей. «Інформація і право». № 2 (21). 2017. С. 88-98.

36. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: http://zakon2.rada.gov.ua/laws/

show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 15.04.2020).

37. Про основи національної безпеки України: Закон України від 19.06.03 р. URL: http://zakon2.rada.gov.ua/laws/show/964-15 (дата звернення: 15.04.2020).

38. Про охорону дитинства: Закон України від 26.04.01 р. № 2402-III. URL:http://zakon3.rada.gov.ua/laws/show/2402-14 (дата звернення: 15.04.2020).

39. Про захист суспільної моралі: Закон України від 20.11.03 р. №1296-IV. URL:http://zakon3.rada.gov.ua/laws/show/1296-15 (дата звернення: 15.04.2020).

40. Про телебачення і радіомовлення: Закон України від 21.12.93 р. № 3759-XII. – URL: http://zakon2.rada.gov.ua/laws/show/3759-12 (дата звернення: 15.04.2020).

41. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.92 р. № 2782-XII. URL: http://zakon3.rada.gov.ua/laws/show/2782-12 (дата звернення: 15.04.2020).

42. Про рекламу: Закон України від 03.07.96 р. № 270/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80 (дата звернення: 15.07.2020).

43. Модельный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»/Принят на тридцать третьем пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (Постановление N 33-15 от 3 декабря 2009 года): URL:http://zakon2.rada.gov.ua/laws/show/997_m85 (дата звернення: 15.04.2020).

44. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V. URL: http://zakon2.rada.gov.ua/laws/show/537-16 (дата звернення: 15.04.2020).

45. Про схвалення Концепції Державної соціальної програми «Національний план дій щодо реалізації Конвенції ООН про права дитини» на період до 2021 року : Розпорядження Кабінету

Міністрів України від 5.04.17 р. № 230-р. URL: http://www.kmu.gov.ua/control/uk/cardnpd?docid=249890555 (дата звернення: 20.04.2020).

46. Панченко О.А., Кабанцева А.В. Державне регулювання інформаційної безпеки дітей. Материалы Международной научно-практической интернет-конференции «Тенденции и перспективы развития науки и образования в условиях глобализации». (28 февраля 2020 г.). Переяслав - 2020. Вып. 56. С. 39-42.

47. Праць О.Є. Ювенальна юстиція: зарубіжний досвід та вітчизняні перспективи. Інтернет-конференція на тему: «Проблеми правової ювеналістики». URL: http://conference.inf.od.ua/index.php/ru/spisok-materialov-konferentsii/sektsiya-4-prava-rebenka-v-sfere-natsionalnogo-prava-i-yuvenalnaya-yustitsiya/59-prots-o-e-yuvenalna-yustitsiya-zarubizhnij-dosvid-ta-vitchiznyani-perspektivi (дата звернення: 20.04.2020).

48. Крестовська Н.М. Ювенальне право України: генезис та сучасний стан : дис. д-ра юрид. наук : 12.00.01. Нац. ун.-т «Одеська юридична академія». О. 2008. 468с.

49. Минимальные стандартные правила ООН, касающиеся отправления правосудия в отношении несовершеннолетних (Пекинские правила). Приняты резолюцией 40/33 Генеральной Ассамблеи Организации Объединенных Наций от 10 декабря 1985 г. URL:jjpk.perm.ru/_res/fs/file6021.doc (дата звернення: 20.04.2020).

50. Закірова С. Ювенальна юстиція в Україні: проблеми, перспективи. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2734:yuvenalna-yustitsiya-v-ukrajini&catid=8&Itemid=350 (дата звернення: 24.04.2020).

51. Белоусов П. Перспективы развития медиации в Украине. Юрист & закон 27.06.2014 – 03.07.2014. № 25. URL: http://www.kisilandpartners.com/content/files/article_belousov_uz_liga_rus.pdf (дата звернення: 20.05.2020).

52. Макаренко Є. Закон про медіацію: нереальна реальність. Юридична Uазетаonline. №38 (640). 18 вересня 2018.

URL: https://yur-gazeta.com/publications/practice/mizhnarodniy-arbitrazh-ta-adr/zakon-pro-mediaciyu-nerealna-realnist.html (дата звернення: 24.05.2020).

53. Директива № 2008/52/ЄС Європейського парламенту і Ради про деякі аспекти посередництва (медіації) в цивільних та комерційних справах. URL: https://zakon.rada.gov.ua/laws/show/994_a95#Text (дата звернення: 24.05.2020).

54. Руководящие принципы Организации Объединенных Наций для предупреждения преступности среди несовершеннолетних (Эр-Риядские руководящие принципы). Приняты резолюцией 45/112 Генеральной Ассамблеи от 14 декабря 1990 года. URL: http://www.un.org/ru/documents/decl_conv/conventions/juveniles_deinquency_prevention.shtml (дата звернення: 20.07.2020).

55. Правила Организации Объединённых Наций, касающиеся защиты несовершеннолетних, лишённых свободы.Приняты резолюцией 45/113 Генеральной Ассамблеи от 14 декабря 1990 года. URL: https://www1.umn.edu/humanrts/instree/Rj1unrjdl.html (дата звернення: 20.05.2020).

56. Рекомендация CM/Rec (2008) 11 Комитета Министров государствам-членам Совета Европы о Европейских правилах в отношении несовершеннолетних правонарушителей, осужденных к наказаниям и мерам уголовно-правового характера (Принята Комитетом Министров 5 ноября 2008 г. на 1040-м заседании заместителей министров). URL: http://www.coe.int/t/dghl/standardsetting/prisons/Prisons_recommendations_ru.pdf (дата звернення: 20.05.2020).

57. Крестовська Н.М. Сім'я та ювенальна юстиція. Молодіжна політика: проблеми та перспективи: зб. наук.праць у 2 вип. Дрогобич: РВВ Дрогобицькогодерж. пед ун-ту імені Івана Франка. 2011. С. 291-294.

58. Навроцький О.О. Забезпечення прав дитини в Україні: теоретичні і практичні засади адміністративно-правового регулювання : автореф. дис. … д-ра юрид. наук : 12.00.07. Хар-

ківський національний університет імені В.Н. Каразіна. Харків. 2018. 36 с.

59. Про Концепцію вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів: Указ Президента України від 10 травня 2006 року. URL: http://zakon2.rada.gov.ua/laws/show/361/2006 (дата звернення: 24.05.2020).

60. Про Концепцію розвитку кримінальної юстиції щодо неповнолітніх: Указ Президента Українивід 24.05.2011 р. №597/2011. URL: http://zakon4.rada.gov.ua/laws/show/597/2011 (дата звернення: 24.05.2020).

61. Про судоустрій і статус суддів: Закон України від 26.04.01 р. № 2402-III. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text (Редакція від 20.06.2020) (дата звернення: 24.05.2020).

62. Питання Уповноваженого Президента України з прав дитини: Указ Президента України від 11 серпня 2011 року №811/2011. URL: https://www.president.gov.ua/documents/8112011-13443 (дата звернення: 24.05.2020).

63. УГОДА ПРО АСОЦІАЦІЮ між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL:https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 24.05.2020).

64. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки: Указ Президента України від 20 травня 2015 року № 276/2015. URL: https://zakon.rada.gov.ua/laws/show/276/2015#Text (дата звернення: 24.05.2020).

65. Проєкт Закону про медіацію. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68877 (дата звернення: 24.05.2020).

66. Крестовська Н.М. Міфи про ювенальну юстицію. Журнал Верховної Ради України «Віче». №15. серпень 2010.

URL: http://www.viche.info/journal/2126/ (дата звернення: 24.05.2020).

67. Закон України "Про попередження насильства в сім'ї" (Відомості Верховної Ради України (ВВР), 2002, N 10, ст.70) URL: http://zakon1.rada.gov.ua/laws/show/2789-14(дата звернення: 24.05.2020).

68. Міжвідомча координаційна рада з питань правосуддя щодо неповнолітніх. Сайт Міністерства юстиції Уаїни. URL: https://minjust.gov.ua/inccojj/about/napryamu_diyalnosti (дата звернення: 24.05.2020).

69. Панченко О.А., Банчук Н.В. Информационная безопасность личности: монография. Киев: КИТ. 2011. 672 с.

70. Баранов О.А. Система принципів інформаційного права. Правова інформатика. 2006. №2 (10). С. 3-13.

71. Ліпкан В. А. Безпекознавство: навч. посібник. Київ: Європ. ун-т. 2003. 208 с.

РОЗДІЛ 5

Медико-психологічні аспекти державного регулювання інформаційної безпеки особистості

5.1. Тривожні розлади людини в умовах турбулентності

Життя особистості в час загальних соціальних трансформацій і потужного інформаційного тиску, які змушують людину перебувати в стані постійного емоційного напруження, стає загальною нормою. Постійний вплив несприятливих факторів (екологічних і соціальних), посилення вимог до певних якостей сприяють прояву тривожності та стресу. Навантаження, що покладається на людську психіку для вирішення цього завдання, часто перевищує її резервні можливості. Подібні умови формують стресовий стан, а довготривале перебування характеризується розвитком хронічного стресу.

У ситуаціях постійних стресів та емоційних навантажень таким проблемам, як от внутрішній неспокій, тривога, дискомфорт, зазвичай не надається належної уваги, попри те, що вони можуть призводити до криз, тяжких душевних потрясінь. У такому стані людина змушена жити, пристосовуючись до довкілля, при цьому її психіка відчуває щодня колосальні навантаження, що найчастіше призводить до емоційно-тривожних, депресивних розладів.

Специфічні стани, що виникають у ситуації невизначеної небезпеки, проявляються в очікуванні несприятливого розвитку подій, що дедалі частіше є штучними та здатні вносити істотні корективи в процесі здійснення турбулентного мислення. Особливо слід виділити взаємозв'язок між турбулентним мисленням і тривожним передчуттям, яке є сутністю підсвідомого рівня з точки зору патофізіології стресу й реакції психіки людини на соціальні виклики.

Сучасне інформаційне середовище є по суті основним джерелом інформації для людини, безпосередньо впливає на її психічну діяльність, на формування її суспільної поведінки. Люди змушені жити в цьому середовищі, адекватно сприймати його реалії з урахуванням інформаційних загроз, яких із часом стає все більше. Серед ризикоутворюючих факторів центральне місце посідає турбулентність інформаційного середовища. Усвідомлення подібних атак спричинило пильну увагу до інформаційної та психологічної безпеки, зокрема удосконалення шляхів її забезпечення. Тому в час суспільних змін проблема психологічної безпеки особистості набуває особливої актуальності, стрімкого розвитку інформаційних технологій, можливостей використання різних засобів впливу на людську свідомість.

Серед авторів, які приділяли увагу проблемі вивчення інформаційної та психологічної безпеки, варто згадати Федорову О.М. [1], Скрипаченко Т.В. [2], Ткачишину О.Р. [3] та ін. У роботах цих авторів досліджувались як окремі аспекти інформаційної безпеки особистості, суспільства, держави загалом, так і окремі питання психологічної безпеки особистості в сучасному інформаційному просторі. Проблематика виникнення й розвитку тривоги також достатньо досліджена. Аналіз феноменології тривоги представлений у роботах Спілбергера Ч.Д. [4], Маслової Т.М., Покацької А.В. [5], Соловйової С.Л. [6], Волошок О.В. [7], Малкової О.Є. [8], Прихожан А.М. [9] та ін. Але актуальним на сьогодні є вивчення виникнення тривожних передчутів у час прогресуючого інформаційно-технічного прогресу.

Інформаційні технології сьогодні є основною загрозою інформаційно-психологічній безпеці особистості. Цій проблемі присвячені дослідження Кузнєцової Ю.М. та Чудової Н.В. [10]. Автори зазначають, що на область Інтернету та інформаційних технологій у цілому проєктуються головні проблеми та страхи суспільства. Дослідження, присвячені проблемам інформаційно-психологічної безпеки й Інтернет-адикції, артикулюють

тривогу колективного несвідомого, беручи на себе тим самим і частину функцій художньої практики. Тому питання психологічної безпеки особистості в епоху турбулентності залишається досить актуальним.

Попередні дослідження турбулентності встановили її багатоаспектність у причинно-наслідковому зв'язку з інформаційною безпекою особистості. Аналіз властивостей інформаційного середовища показав, що турбулентність у синергетиці з іншими її характеристиками є деструктивним фактором інформаційно-психологічної безпеки як у відношенні до держави та суспільства, так і окремої особистості. Під інформаційно-психологічною безпекою мається на увазі стан захищеності окремих осіб і (або) груп осіб від негативних інформаційно-психологічних впливів та пов'язаних із цим інших життєво важливих інтересів особистості, суспільства й держави в інформаційній сфері.

При дослідженні шляхів подолання турбулентності через призму властивостей особистості введено поняття «інформаційно-психологічна турбулентність» – нестабільний стан психіки людини, викликаний інформаційним впливом, що виявляється в раптових припливах гніву, печалі або відчаю, відчутті тривоги, роздратуванні, страху чи смутку [7].

В. Франкл [11] зазначав, що для повноцінного існування людини важливим є її смислові цінності. Чітке розуміння життєвих цінностей сприяє формуванню характеру, контролю дій, бажань і, звичайно ж, рішень. Смислові цінності можна поділити на три групи: цінності творчості, цінності переживання та цінності відносин. Пріоритет належить цінностям творчості, основним шляхом реалізації яких є праця та професійна діяльність. Із числа цінностей переживання В. Франкл найбільше значення надає любові, яка має життєстверджуючий потенціал. До цінностей відносин людині доводиться вдаватися, коли вона виявляється під владою обставин, що не в змозі змінити. Але за будь-яких обставин людина здатна зайняти осмислену позицію по відношенню до них і надати своєму стражданню глибокий

сенс. І як наслідок тривога – занепокоєння, страх, паніка, жах. Це ті явища, які присутні в нашому психічному житті в часи неспокійного сьогодення. Вони можуть бути різними за інтенсивністю, тривалістю, структурою від легкого короткочасного неспокою до паралізуючого жаху, складаючи різноманітну гаму переживань, що супроводжують найрізноманітніші життєві події: хвороби, конфлікти, утрату роботи, зокрема доходу, неприємні й несподівані події.

Емоція тривоги – одне з найбільш частих переживань людей у критичних ситуаціях, яке при надзвичайних впливах може виконувати різні функції – як адаптивну, так і дезорганізуючу психічну діяльність. У сучасній психіатрії та психології прийнято розрізняти поняття «тривога» та «тривожність» через категорії психічного стану й психічної властивості, хоча в англійській мові вони позначаються одним словом – anxiety. Тому, читаючи іноземну літературу, для розведення понять треба звертати увагу на контекст їхнього застосування.

Поняття тривоги було введено в психологію З. Фрейдом, який розводив страх на конкретний страх (нім. Furcht) і невизначений, підсвідомий страх – тривогу, що носить глибинний, ірраціональний, внутрішній характер (нім. Angst). Тривога розглядається в психології як несприятливий за своїм емоційним забарвленням стан або внутрішня умова, яка характеризується суб'єктивними відчуттями напруги, невизначеності, занепокоєння, очікування негативних подій, похмурих передчуттів. На відміну від страху, тривога зазвичай паралізує почуття, пов'язана з підсвідомою мобілізацією психічних сил організму для подолання потенційно небезпечної ситуації. Страх, навпаки, спонукає людину до неусвідомленої дії, призводить до руху [12].

Багатьма дослідниками зазначено, що стан тривоги може варіюватися за інтенсивністю та змінюватися в часі як функція рівня стресу, якому піддається людина. Аналізуючи «яскравість» переживання тривоги, Ф.Б. Березін (1988) виділив у ньому шість рівнів та об'єднав їх назвою «явища тривожного ряду».

1. Тривозі найменшої інтенсивності відповідає відчуття внутрішньої напруженості, що виражається в переживаннях напруженості, настороженості, дискомфорту. Воно не несе в собі ознак загрози, однак служить сигналом наближення більш виражених тривожних явищ. Даний рівень тривоги має найбільше адаптивне значення.

2. Відчуття внутрішньої напруженості змінюється або доповнюється реакціями гіперостезії, завдяки яким раніше нейтральні стимули набувають значимості, а при посиленні – негативних емоційних забарвлень (на цьому заснована дратівливість).

3. Наступний рівень – це власне тривога, що проявляється в переживанні невизначеної загрози, відчутті неясної небезпеки, яке може перерости в страх.

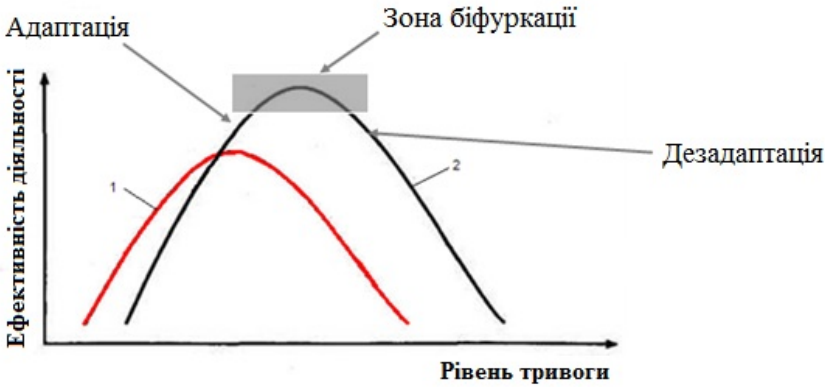
4. Стан, що виникає при наростанні тривоги та проявляється в опредметненні невизначеної небезпеки. При цьому об'єкти, ідентифіковані як «лякаючі», необов'язково зображують реальну причину тривоги.

5. Відчуття невідворотності насування катастрофи, що виникає в результаті наростання тривоги й переживання неможливості уникнути небезпеки, неминучої катастрофи, що пов'язано не зі вмістом страху, а лише з наростанням тривоги.

6. Найбільш інтенсивний прояв тривоги – тривожно-боязке порушення, яке виражається в потребі в руховій розрядці, пошуку допомоги, що максимально дезорганізує поведінку людини.

П'ятий рівень слід віднести ще до передклінічного прояву тривоги, тоді як шостий вже підпадає під класифікацію МКБ-10 (F40-F41).

Відповідно до теорії перевернутого U, що спирається на відомий закон Йеркса-Додсона, тривога до певної міри може стимулювати діяльність, але, подолавши рубіж «зони оптимального функціонування» індивіда, починає виробляти розслаблюючий–дезорганізуючий ефект (Ю.Л. Ханін, рис. 5.1.) [13].



Примітка: 1 – «Висока» тривожність; 2 – «Низька» тривожність

Рис 5.1. Закон Йеркса-Додсона

Такий ефект має тільки інтенсивна тривога, що має дезорганізуючий вплив на діяльність, це вкрай несприятливий для людини стан, що вимагає подолання або трансформації. Для психологів саме вона представляє найбільший інтерес, оскільки цей вид тривоги в суб'єктивному досвіді людини є «проблемним».

Таким чином, стан тривоги виникає як функція (потенційно) небезпечної ситуації та особистісних особливостей людини, пов'язаних із її інтерпретацією. Ми вважаємо також, що точка «перелому» (біфуркації) (рис. 5.1.) настає тим швидше, чим вищий рівень турбулентності ІС.

Тривожність виступає як значення функції (рис. 5.1.), безпосередньо не виявляється в поведінці, але її рівень можна визначити виходячи з того, як часто й наскільки інтенсивно в людини спостерігаються стани тривоги. Особистість із вираженою тривожністю схильна сприймати навколишній світ як такий, що містить у собі небезпеку й загрозу значно більшого ступеня, ніж особистість із низьким рівнем тривожності [4].

Стан тривоги, як і будь-який інший негативний психічний стан, знаходить своє вираження на різних рівнях людської організації:

– на фізіологічному рівні – тривога проявляється в посиленні серцебиття, прискоренні дихання, підвищенні артеріального тиску, збільшенні хвилинного обсягу циркуляції крові, появі сухості в роті, зростанні загальної збудливості, зниженні порогів чутливості, слабкості в ногах та іншому;

– на емоційно-когнітивному рівні – характеризується переживанням безпорадності, незахищеності, безсилля, амбівалентності почуттів, що породжує труднощі в ухваленні рішень і досягненні цілей;

– на поведінковому рівні – безцільне ходіння по приміщенню, гризіння нігтів, стукіт пальцями по столу, хитання на стільці, крутіння в руках різних предметів, перебирання волосся і т.ін.

На відміну від тривоги, тривожність у сучасній психології розглядається як психічна властивість, індивідуальна психологічна особливість, що виявляється у схильності людини до переживання тривоги. Тривожність безпосередньо не виявляється в поведінці, але її рівень можна визначити виходячи з того, як часто і як інтенсивно в людини спостерігається стан тривоги. Особистість із вираженою тривожністю схильна сприймати навколишній світ, що містить у собі небезпеку й загрозу в значно більшому ступені, ніж особистість із низьким рівнем тривожності [4].

Сучасний підхід до феномену тривожності ґрунтується на тому, що останню не слід розглядати як початкову негативну рису особистості; вона являє собою сигнал неадекватності структури діяльності суб'єкта стосовно до ситуації. У сучасній науці тривожність розглядається як один із основних параметрів індивідуальних відмінностей. Для кожної людини характерний свій оптимальний рівень тривожності, так звана корисна тривожність, яка є необхідною умовою розвитку особистості. Фахівці вважають, що, швидше за все, в одних людей існують генетично обумовлені передумови до формування тривожності, у той час як у інших дана психічна властивість є придбаною індивіду-

альним життєвим досвідом. При цьому приналежність тривоги до того чи іншого рівня психічної організації людини досі залишається спірним питанням; її можна трактувати і як індивідуальну, так і як особистісну властивість людини.

Існують різні форми тривожності, тобто особливі способи її переживання, усвідомлення, вербалізації й подолання, серед яких можна виділити наступні варіанти переживання та подолання тривожності [9]:

– особистісна тривожність – це стійка індивідуальна характеристика, що визначає схильність людини до тривоги. Такий вид тривожності активізується при сприйнятті людиною ситуацій, які вона розглядає як небезпечні, загрозливі її престижу, самооцінці, самоповазі. При високому рівні особистісної тривожності необґрунтовано широке коло об'єктивно безпечних обставин сприймається людиною як загрозливе, викликаючи реакції, інтенсивність яких не відповідає величині реальної небезпеки;

– ситуативна тривожність – це стан, що характеризується емоційними переживаннями, такими як напруженість, занепокоєння, заклопотаність, нервозність. Подібні стани виникають як емоційна реакція на конкретну зовнішню стресову ситуацію. Така тривожність може бути різною за інтенсивністю й за часом протікання. Дуже висока ситуативна тривожність викликає порушення уваги, а також тонкої координації.

Таким чином, і тривога, як психічний стан, і тривожність, як психічна властивість, знаходяться в конфронтації з базовими особистісними потребами: потребою в емоційному благополуччі, почутті впевненості, безпеки. Те ж саме можна сказати про інформаційно-психологічну турбулентність, що характеризується подібними явищами. У таблиці 5.1. наведено параметри, що дозволяють оцінити відмінність і схожість тривоги й інформаційно-психологічної турбулентності з психологічної точки зору.

Таблиця 5.1.

Порівняльні риси тривоги й інформаційно-психологічної турбулентності

Параметр	**Тривога**	**Інформаційно-психологічна турбулентність**
Специфіка	Психічний стан, що характеризується переживанням невиразної (неясної) небезпеки.	Психічний стан, що характеризується хаотичністю мислення, панічними атаками та іншими деструктивними реакціями.
Етіологія	Невизначена або загрозлива ситуація; дефіцит інформації або її надлишок. Незадоволеність соціально-психологічних потреб.	Турбулентний вплив інформаційного середовища (інформаційна та суспільно-політична турбулентність); загроза інформаційній безпеці.
Можливі деструктивні прояви	Порушення когнітивних функцій, функціонування психічних процесів і соціалізації; саморуйнівної поведінки (шкідливі звички, аддикції у вигляді невротичних і неврозоподібних розладів соматоформного типу (МКБ-10 F 4).	Порушення критичності мислення, сприйняття, неадекватна оцінка подій. Девіантна й делінквентна поведінка.
Позитивний результат	Адаптація.	Адаптація. Турбулентне мислення.
Негативний результат	Дезадаптація. Дистрес. Психічні та психосоматичні розлади. Зміна особистості.	

Аналізуючи рисунок 5.1. і таблицю 5.1, припустимо, що, по-перше, точка біфуркації настає тим швидше, чим вищий рівень турбулентності ІС; по-друге, ефективність діяльності особистості поблизу зазначеної точки визначається нелінійною поведінкою рівня тривоги в силу неусвідомлених інформаційних загроз, тобто в цьому місці виявляється турбулентний стан психіки (неможливо точно сказати, чи є тривога стимулюючим або розслаблюючим фактором), і, відповідно, тривога має схожі ознаки з інформаційно-психологічною турбулентністю.

Тривожне передчуття визначаємо як спонтанний емоційний сплеск у результаті та на фоні стану тривоги, причина якої витіснена на рівень підсвідомого.

Тривожне передчуття може виступати в наступних проявах:

– прекогніція – трансперсональне переживання, у ході якого відбувається отримання або обробка інформації про майбутнє;

– інтуїція – інтуїтивне передчуття, що супроводжується відчуттями занепокоєння очікування до самого факту звершення події;

– фобія – страх, суттю якого є ірраціональний неконтрольований страх або стійкий тривожний стан.

Зазначені прояви відрізняються «яскравістю» та силою відчуттів, але в будь-якому випадку вони надані природою для того, щоб особистість змогла запобігти загрозливій події, ужившиконкретні превентивні заходи.

Так, когнітивне передчуття, до володіння яким здатні тільки окремі особистості (здатність знати, що, коли і як відбудеться), можна використовувати не тільки для своєї, а й для безпеки на рівні суспільства й держави.

Розвинена інтуїція дає можливість не тільки розпізнати небезпечну ситуацію, але й знайти шляхи виходу з неї. По суті, інтуїція це результат процесу обробки інформації, що надходить

до підсвідомості надвисокою швидкістю, таким чином знання, що виникає без усвідомлення шляхів і умов його отримання, «не вкладається» в логічні рамки.

Фобія часто пов'язана з перевтомою, стресом, виснаженням нервових процесів і т.ін. Вона сигналізує про те, що людині, перш за все, потрібно перестати ігнорувати себе і свої реакції на те, що відбувається. Необхідно ірраціональний страх «перемістити» в усвідомлений страх реальної загрози, із яким зрозуміло, як боротися й знаходити вихід із ситуації.

Фобія як найслабший стан психіки знаходиться в причинно-наслідковому зв'язку з інформаційно-психологічною турбулентністю, а прекогніція та інтуїція – із турбулентним мисленням. Взаємозв'язок описуваних явищ психіки відображений на рис. 5.2.

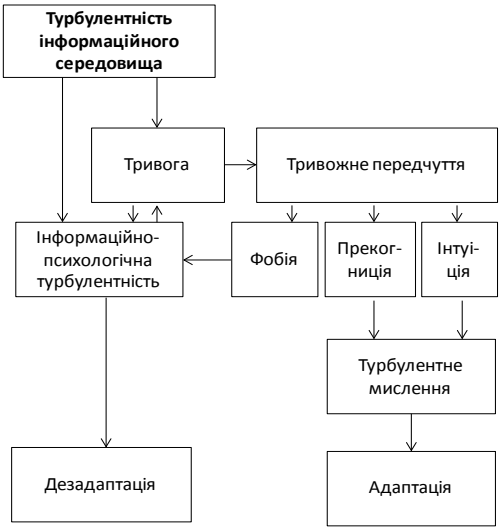


Рис. 5.2. Взаємозв'язок тривоги та турбулентності

Невизначеність інформаційного середовища виступає як деструктивний чинник, формуючи шари інформаційної та суспільно-політичної турбулентності, і як наслідок потраплян-

ня особистості до іформаційно-психологічної турбулентності. Перебування особи в стані інформаційно-психологічної турбулентності веде до виникнення постстресових розладів, що вимагає адекватного медико-психологічного реагування.

Дані моніторингу [12] підкреслюють необхідність розробки нових підходів медико-психологічної допомоги, яка полягає в зниженні тривоги та підвищенні адаптації до нових умов існування із застосуванням комплексних медико-психологічних заходів на державному рівні.

Необхідно використовувати диференційований підхід до діагностики психічних розладів унаслідок військових конфліктів, інформаційно-психологічних війн, як основних загроз державі, суспільству, населенню. Проблема надання спеціалізованої допомоги населенню має два важливих і принципових аспекти: психологічний і власне психіатричний, що обумовлює необхідність комплексного підходу із залученням різноманітних фахівців суміжного профілю (психологів, психотерапевтів та ін.). Саме такий підхід здатний забезпечити не тільки своєчасну адекватну медико-психологічну допомогу, а й провести адресні психопрофілактичні та психокорекційні заходи, спрямовані на зниження тяжкості та вираженості психологічних, психічних і психосоматичних наслідків під час ведення бойових дій, а також у найближчі та віддалені періоди після їх завершення.

Сучасні турбулентні явища формують тривожні передчуття серед населення, тим самим спричиняючи загрозу національній безпеці держави. Забезпечення інформаційної безпеки сприятиме формуванню повноцінно-ціннісного потенціалу як окремої особистості, так і держави загалом. Психологічна безпека особистості проявляється, з одного боку, у її здатності зберігати стійкість в інформаційному середовищі з певними параметрами, а також із різними психотравмуючими впливами в опорі деструктивним внутрішнім і зовнішнім впливам, з іншого боку – в емоційній експресивності, інтелектуальній, поведін-

ковій варіативності, оптимальній позиції суб'єкта в умовах інформаційного середовища.

Тому турбулентні процеси в державі, тобто їхнє прогнозування, своєчасне виявлення, робота по запобіганню та нівелюванню турбулентних викликів є основою інформаційно-психологічного благополуччя особистості в державі та її плідного розвитку.

5.2. Медико-психологічний супровід пацієнтів із тривожними розладами

На сьогоднішній день тривожні розлади набули особливого значення. Практично кожна людина зіштовхувалася з тривожними переживаннями у своєму житті. Проблема тривожних розладів обумовлена низкою факторів: у структурі психічної патології тривожні розлади є другими за поширеністю після розладів настрою; тривожні розлади в рамках психічної патології відзначаються при ендогенній, екзогенній і органічній патології. Їхня поширеність у структурі психічної патології від 6 до 13,6%; дезадаптаційний вплив на соціальне функціонування, працездатність і в цілому на якість життя [14]. Своєчасне виявлення та надання професійної допомоги обумовлено ранньою діагностикою, попередженням психосоматичних розладів і збереженням здоров'я нації.

Деструктивні чинники гібридної (інформаційно-психологічної) війни, що все частіше виникають останнім часом, можуть викликати стійкі зміни в людей із низьким рівнем стресостійкості, тим самим послаблюючи кадровий потенціал держави й систему національної безпеки загалом. Нервова система відчуває постійний тиск і може залишатися постійно в активному стані, що стимулює продовження вироблення додаткових порцій гормонів стресу протягом тривалого періоду. Це виснажує резерви організму, викликає в людини відчуття перевтоми й слабкості. Послаблюється імунна система організму, виника-

ють інші проблеми, пов'язані з вичерпанням різних біологічних резервів. Стрес часто викликає формування різних психічних розладів, одним із яких є невротична тривога (панічний розлад).

Як зазначає Л.М. Юр'єва, тривога може бути нормальною, патологічною, фармакогенною [15] (рис. 5.3.)

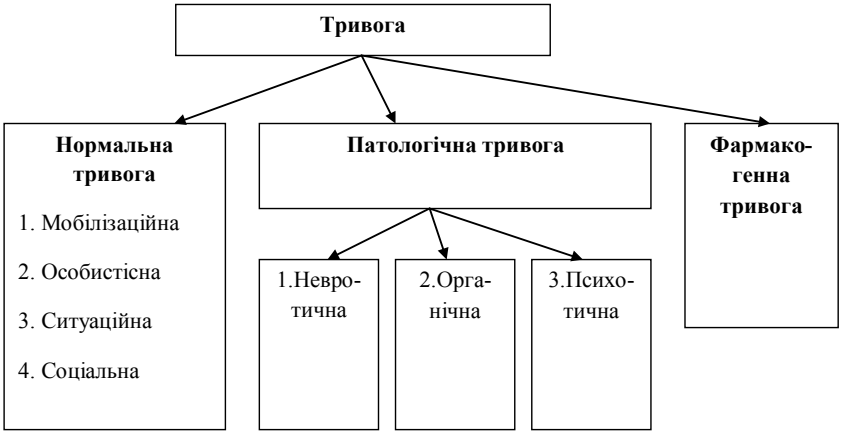


Рис. 5.3. Типологія тривоги

Нормальна (адаптаційна) тривога пропорційна об'єктивній небезпеці та є найважливішим адаптаційним механізмом людини. Вона має профілактичне значення, бо постійно сигналізує людині про небезпеку й спонукає її до дій, які вона здійснює у силу того, що постійно прагне до емоційного гомеостазу. Ця тривога, як правило, нетривала, помірна і не порушує продуктивної діяльності людини. До даного виду тривоги відносяться наступні підвиди:

1. Мобілізаційна тривога. Виникає епізодично та сприяє мобілізації фізичних і психічних ресурсів людини. Характерна для психічно здорових, вольових, активно діючих особистостей;

2. Особистісна тривога або тривожність. Є відносно стабільною особистісною характеристикою й рисою характеру, яка

визначає поріг виникнення реакції тривоги. Низький поріг характерний для тривожних, ананкастних і залежних акцентованих особистостей;

3. Ситуаційна тривога – стан тривоги, що виникає тільки при стресовій ситуації і припиняється по її завершенню;

4. Соціальна тривога – тривога, виникає при взаємодії із соціумом (публічних виступах і діях, спілкуванні з чиновниками й керівниками та ін.). Ці люди надмірно стурбовані думкою оточуючих про себе, бояться негативних оцінок і відкидання. Чим вищий рівень тривожності, тим нижчий показник життєвого задоволення. Якщо ці розлади не досягають ступеня клінічно оформленого стану з вегетативними, психологічними й поведінковими розладами та суттєво не порушують адаптацію, то вони розцінюються в рамках «нормальної» тривоги. Якщо ці розлади клінічно оформлені, то вони розцінюються в рамках патологічної тривоги (соціальна фобія F40.1).

У деяких випадках при нормальній тривозі необхідна консультація психолога, аутотренінг. Особи з ситуаційною та соціальною тривогою є цільовою групою для первинної профілактики й психоосвітніх програм.

Патологічна тривога за своєю інтенсивністю й тривалістю не корелює із реальною загрозою та являє собою психічний розлад (невротичного або психотичного рівня). Патологічна тривога може бути причиною або пусковим механізмом як психічних, так і соматичних захворювань. Це генералізована реакція організму, що виявляється вегетативними, психологічними й поведінковими симптомами. До цієї категорії тривоги належать:

1. Невротична тривога – клінічно оформлений стан тривоги, що виникає в результаті соціальних і психологічних стресів та ситуацій, які не становлять небезпеки на даний час. Вона позбавляє людину здатності до нормальної життєдіяльності. Відзначають високу коморбідність невротичної тривоги із депресією, що може потенціювати суїцидальну небезпеку таких пацієнтів. Ризик суїцидальної поведінки в осіб із невротичними

й пов'язаними зі стресом розладами в цілому в 3 рази вищий, ніж у популяції. Найбільшу суїцидальну небезпеку серед цієї групи розладів становлять особи із посттравматичним стресовим розладом, генералізованим тривожним і панічним розладами, де ризик суїцидальних спроб перевищує такий у популяції в 6 разів. У МКБ-10 ці стани класифікуються як:

- панічний розлад;
- генералізований тривожний розлад;
- синдром нав'язливих станів (обсесивно-компульсивний розлад);
- соціофобія (або соціально тривожний розлад);
- специфічні фобії;
- змішаний тривожний і депресивний розлад;
- тривожно-фобічні розлади.

Панічний розлад. Приступ панічної атаки є раптовим дискретним, коротким періодом інтенсивного дискомфорту, тривоги або страху, що супроводжується соматичними та / або когнітивними симптомами. Панічний розлад проявляється у вигляді виникнення повторних панічних нападів, як правило, супроводжується побоюваннями з приводу майбутніх нападів або змінами в поведінці, щоб уникнути ситуацій, які можуть призвести до нападів. Панічний розлад часто супроводжується іншими серйозними захворюваннями, такими як депресія, наркоманія чи алкоголізм. При депресії людина відчуває стан пригніченості або безнадійності, порушення апетиту або сну, знижений рівень енергії та труднощі з концентрацією.

Генералізований тривожний розлад – характеризується надмірною тривогою й занепокоєнням із приводу різних життєвих ситуацій або подій, що присутні понад ≥ 6 міс. Фокус занепокоєння не обмежений, як при інших психічних розладах (наприклад, панічні напади розвиваються в громадських місцях); пацієнт має кілька тривожних його причин, які часто з часом змінюються. До їхньої кількості відносяться ситуації на роботі, у сім'ї, фінансове забезпечення, здоров'я, безпека й т. ін. Хви-

лювання, як правило, супроводжується наступними проявами: рухове занепокоєння, збудженість або нервозність, легка стомлюваність, труднощі з концентрацією уваги, дратівливість, напруга м'язів, тривожний сон.

Синдром нав'язливих станів (обсесивно-компульсивний розлад). Люди, які страждають цим синдромом, переживають наполегливі неприємні думки (нав'язливі думки) і використовують ритуали (компульсивні дії), щоб контролювати тривогу, викликану саме цими думками. У рівній мірі страждають чоловіки та жінки, і зазвичай розлад проявляється в дитинстві, юнацтві або ранньому дорослому віці [16]. В однієї третини дорослих, які страждають ОКР, симптоми з'явилися в дитинстві. Дані досліджень говорять про те, що ОКР може бути спадковим захворюванням [17]. У більшості випадків усе закінчується тим, що ритуали починають контролювати життя людини. Наприклад, якщо людина одержима страхом бактерій і бруду, у неї виробляється компульсія весь час мити руки. Якщо в неї розвивається нав'язливий страх, що хтось може проникнути до будинку, то перед тим, як лягти спати, вона багато разів закриває й перевіряє ще раз замки.

Соціофобія (соціальний тривожний розлад). Цей діагноз ставлять у тих випадках, коли людина стає надмірно тривожною, занадто сором'язливою або затиснутою в повсякденних соціальних ситуаціях. Люди з соціофобією відчувають постійний, сильний, хронічний страх, що на них дивляться та за ними спостерігають, страх осуду й боязнь опинитися в незручному становищі. Вони можуть турбуватися протягом днів або тижнів через подію, якої вони бояться. Цей страх може бути настільки сильним, що стає на заваді в роботі, навчанні та інших повсякденних справах, ускладнює нові знайомства та ставить під загрозу стару дружбу. І хоча хворі на соціофобію розуміють, що їхній страх перебувати поруч із людьми недоречний і необґрунтований, вони все ж не в змозі подолати його. Навіть якщо їм удається подолати страх і вийти на люди, вони зазвичай шале-

но хвилюються напередодні заходу, відчувають себе вкрай некомфортно й під час та годинами по його завершенню переживають, що про них скажуть. До фізичних симптомів, які часто супроводжують соціофобію, відносяться: почервоніння, сильна пітливість, тремтіння, нудота та труднощі під час розмови.

Специфічні фобії – це сильний страх перед чимось, що насправді не представляє собою великої небезпеки або є зовсім безпечним. Деякі з найбільш поширених специфічних фобій: боязнь закритого простору, висоти, ескалаторів, тунелів, їзди по шосе, води, польотів, собак і крові. Такі фобії – це не просто сильний страх; це – ірраціональний страх чогось конкретного. Незважаючи на те, що дорослі люди, які страждають фобіями, розуміють, що їхні страхи ірраціональні, зустріч або навіть думка про зустріч із об'єктом, який уселяє страх або ситуацію, провокує напад паніки або сильної тривоги.

Змішаний тривожний і депресивний розлад. Ця категорія використовується, коли присутні симптоми як тривоги, так і депресії, але ні одні, ні інші окремо не є чітко домінуючими або вираженими настільки, щоб виправдати діагноз. Крім того, мають місце деякі вегетативні симптоми: тремор, серцебиття, сухість у роті, бурління в животі й т.ін.

Тривожно-фобічні розлади – група розладів, у якій тривога викликається виключно або переважно певними ситуаціями або об'єктами (зовнішніми по відношенню до суб'єкта), які на даний час не є небезпечними. У результаті ці ситуації уникаються або переносяться з почуттям страху. Фобічна тривога суб'єктивно, фізіологічно й поведінково не відрізняється від інших типів тривоги та може відрізнятися за інтенсивністю від легкого дискомфорту до жаху. Стурбованість пацієнта може концентруватися на окремих симптомах, таких як відчуття нудоти, і часто поєднується із вторинними страхами смерті, утрати самоконтролю чи божевілля. Тривога не зменшується від свідомості того, що інші люди не вважають цю ситуацію такою небезпечною або загрозливою. Одне лише уявлення про попадання в фобічну си-

туацію зазвичай заздалегідь викликає тривогу передбачення. Фобічна тривога часто співіснує з депресією.

2. Органічна тривога. Тривога виникає як наслідок органічних причин: патології серцево-судинної системи, органічних уражень ЦНС, патології щитовидної і паращитовидної залоз, недостатності вітаміну В12, гіпоглікемії та інших. Поведінкові особливості тривоги найчастіше проявляються у вигляді метушливості, дратівливості, емоційної лабільності, дезорганізації діяльності, нездатності розслабитися, уникнення стресових ситуацій. Серед психологічних проявів тривоги переважають почуття пригніченості, безпорадності, невпевненості, знижена самооцінка, комплекс провини та неповноцінності.

3. Психотична тривога. Часто передує першому психотичному епізоду, рецидивам шизофренії, шизоафективних психозів. Вона є тригером гострих афективно-маячних нападів, гострого почуттєвого марення, онейроїдних станів. Тривога в рамках тривожно-параноїчної і тривожно-депресивної симптоматики є фактором ризику скоєння суїциду. Пацієнти з психотичною тривогою потребують психіатричної допомоги (у гострому періоді – стаціонарної). У терапії питому вагу займає фармакотерапія (нейролептики, антидепресанти). Після редукції психотичних проявів можлива психотерапевтична корекція і проведення психосоціальної терапії.

Проблема панічних розладів в останні роки, характерні гібридними війнами, стає все більш актуальною. Військові дії на Сході України призвели до значного морального й матеріального збитку для регіону та країни в цілому. Усе більша кількість військовослужбовців залучається до вирішення цих конфліктів, страждає мирне населення. Гостро стоїть проблема впливу травмуючих подій на психічне здоров'я населення, яке проживає на території проведення операції об'єднаних сил.

Практика показує, що цивільне населення, яке мешкає у зоні локальних війн, не менше, ніж учасники бойових дій, пере-

живає важкі психічні травми, які викликають відповідний рівень психічних розладів.

Специфіка даної проблеми, її багатогранність і різноманітність соціальних, психологічних, біологічних і медичних умов, проявів визначає багатокомпонентний підхід до її вивчення. Слід підкреслити необхідність і важливість психологічних досліджень для виявлення клініко-психопатологічних особливостей розладів психіки та поведінки в населення й розробки ефективних методів лікування, психокорекції та психологічної реабілітації постраждалих.

Відомо, що психогенний вплив травмуючих подій складається не тільки з прямої безпосередньої загрози життю людини у зв'язку з її очікуванням, а також із різними індивідуально-значущими наслідками. Психогенні розлади, причини їх виникнення, клініко-психопатологічні особливості, динаміка залежать від сукупності психотравмуючих чинників, а також від індивідуально-особистісних характеристик. Психологічна стійкість може залежати від організованості та узгодженості дій оточуючих, їхньої підтримки.

Війна, із точки зору екстремальних умов, сприяє виникненню психогеній, об'єднує по суті психотравмуючі фактори, властиві майже всім стихійним лихам і катастрофам. У зв'язку з почастішанням цих подій і підвищенням уваги суспільства до психічного стану населення, що знаходиться в критичних ситуаціях, особливе місце в психіатричній практиці сучасності посіли посттравматичні психічні розлади [18]. При цьому динамічний психопатологічний аналіз свідчить про стереотип розвитку непсихотичних психічних розладів: від реакції адаптації до невротичних реакцій, виникнення невротичного стану та патохарактерологічного (невротичного) розвитку особистості [19].

Специфіка даної проблеми, її багатогранність і різноманітність соціальних, психологічних, біологічних і медичних умов, проявів визначає багатокомпонентний підхід до її вивчення. Слід підкреслити необхідність і важливість психологічних

досліджень для виявлення клініко-психопатологічних особливостей розладів психіки та поведінки в населення, розробки ефективних методів лікування, психокорекції та психологічної реабілітації постраждалих, що є важливим державним завданням.

Із 2014 по 2019 рр. на базі державного закладу «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України» (ДЗ «НПМ РДЦ МОЗ України») проводилося психодіагностичне обстеження жителів регіону з метою виявлення клініко-психопатологічних особливостей розладів психіки та поведінки. У період проведення дослідження виконувалися науково-дослідні роботи за запитом МОЗ України: «Діагностика, лікування та реабілітація посттравматичних стресових і тривожних розладів, обумовлених соціальностресовими факторами, у населення в зоні проведення антитерористичної операції» (№ держреєстрації 0115U002757, термін виконання 2015-2017 рр.), «Розробка системи медико-психологічної допомоги дітям та підліткам, що перебувають у зоні проведення антитерористичної операції» (№ держреєстрації 0116U004162, термін виконання 2016-2018 рр.), «Тривога й пов'язані з нею психічні, психосоматичні та соматичні розлади в населення в зоні проведення антитерористичної операції» (№ держреєстрації 0118U004166, термін виконання 2018-2019 рр.).

У дослідженні взяли участь: доросле населення, яке мешкає в зоні військового конфлікту, – 3017 осіб та дитячий контингент – 1695 дітей. Групу дорослих склали 72,3% жінок і 27,7% чоловіків, у яких переважала середньо-спеціальна та вища освіта. У таблиці 5.2. представлено психодіагностичний комплекс для дорослої групи осіб із досліджуваними показниками.

Таблиця 5.2.

Психодіагностичний комплекс дослідження

Психологічний інструментарій	Досліджувані показники
• Авторська анкета • Опитувальник «Способи копінг-поведінки» Р. Лазаруса; • Опитувальник вираженості психопатологічної симптоматики (Symptom Check List-90-Revised - SCL-90-R) Дерогатіса, • Стандартизований багатофакторний метод дослідження особистості СМІЛ, • Міссісіпська шкала посттравматичного стресового розладу ПТСР, • Шкала психологічного благополуччя К. Ріфф, • «Метод колірних виборів Люшера», • Методика вимірювання рівня тривожності Тейлора; • Шкала астенічного стану (Малкова Л.Д.); • Інтегративний тест тривожності (Бізюк А.П., Вассерман Л.І., Іовлев Б.В.) • Шкала базисних переконань • Індивідуально-типологічний опитувальник Л.М. Собчик - шкала агресивності, • Таблиці Горбова • Опитувальник суїцидального ризику (Розуваєвої Т.М.)	• Копінг-стратегії • Тривожність, фобічна тривожність • Соматизація • Депресія • Ворожість • Особистісні особливості • ПТСР • Механізми психологічного захисту • Психологічне благополуччя • Рівень емоційної напруги • Ступінь астенічного стану • Доброзичливість навколишнього світу • Агресивність • Когнітивно-пізнавальна сфера • Порушення сну, зниження активності, зниження інтересу до значущих видів діяльності • Злам культурних бар'єрів • Афектність • Соціальний песимізм • Антисуїцидальний фактор

У ДЗ «НПМ РДЦ МОЗ України» розроблена система безперервного маршруту пацієнта від комплексної діагностики, лікування, реабілітації до оцінки ефективності проведених заходів (рис. 5.4.).

Рис. 5.4. Система маршрутизації пацієнтів із постстресовими розладами

У реєстратурі медреєстратор оформляє медичну документацію у формі медичної картки, куди вносить персональні дані про пацієнта (прізвище, ім'я, по батькові, стать, дата народження, місце роботи, адреса проживання, паспортні дані та контактна інформація) і направляє до кабінету долікарського контролю. У кабінеті долікарського контролю медична сестра проводить попереднє обстеження (візуальний огляд, вимірювання артеріального тиску, температури, збір скарг, фіксацію висловлювань пацієнта з приводу проблем, які його турбують за станом здоров'я та емоційного забарвлення) і коротке анкетування із подальшим направленням до кабінету психолога.

Пацієнт із направленням звертається за консультацією до психолога у відділенні медичної та соціальної психології. Психолог проводить скринінгове психодіагностичне дослідження з метою виявлення особливостей психоемоційного стану і визначення «групи ризику», до якої входять пацієнти з психологічними проявами ПТСР, із високими показниками за шкалами тривожності (соматизація, депресія, агресія, порушення когнітивно-пізнавальних процесів та інше).

У разі виявлення пацієнта «групи ризику» психолог рекомендує консультацію психіатра. Психіатр консультує та дає свої рекомендації. За необхідності (за показаннями) долучаються інші вузькопрофільні спеціалісти. За результатами проведеного консультативно-діагностичного етапу складається індивідуальна програма багатокомпонентного лікування та реабілітації пацієнтів зі встановленою патологією, що включає фармакотерапію, психотерапію, фізіотерапію. Багатокомпонентна модель реабілітації (відновлення) реалізується узгодженням зусилля команди професіоналів різного профілю (психіатр, невропатолог, фізіотерапевт, ерготерапевт, психолог, рефлексотерапевт, терапевт, кардіолог, ендокринолог, сестра медична). Склад бригади професіоналів варіюється залежно від наявних проблем і виявленої патології у пацієнта.

За результатами проведеного первинного анкетування дорослої групи були виявлені рівні емоційного, фізичного стану та працездатності. Так, свій емоційний стан оцінили як гарний 26,5% респондентів, задовільний – 40,5%, незадовільний – 33% респондентів. Фізичний стан оцінили як гарний 26,5% респондентів, задовільний – 42%, незадовільний – 32,5% респондентів. Гарний рівень працездатності відзначили 27% респондентів, задовільний рівень працездатності – 44,5%, незадовільний – 28,5% респондентів.

Дослідження ситуативної тривожності за методикою «Інтегративний тест тривожності» (Бізюк А.П. Вассерман Л.І., Іовлев Б.В.) надало змогу дослідити прояви тривожності за різними компонентами (табл. 5.3.).

Результати кореляційного аналізу показали статистично значущі кореляційні зв'язки між особистісною та ситуативною тривожністю ((rs=0,718), (p<0,05)). Результати дослідження рівня особистісної тривожності представлені в таблиці 5.4.

Таблиця 5.3.

Прояви тривожності серед населення

Вид тривожності	Ситуативна тривожність	Особистісна тривожність
Емоційний дискомфорт		
низький рівень тривоги	48,5%,	30,5%,
нормальний рівень тривоги	33%	44%
високий рівень тривоги	18,5%	25,5%.
Астенічний компонент		
низький рівень тривоги	45,5%	30%
нормальний рівень тривоги	39,5%	34%
високий рівень тривоги	15%	36%
Фобічний компонент		
низький рівень тривоги	27,5%,	9%
нормальний рівень тривоги	41%	39,5%
високий рівень тривоги	31,5%	51,5%
Тривожна оцінка перспектив		
низький рівень тривоги	54,5%	19%
нормальний рівень тривоги	27,5%	52%
високий рівень тривоги	18%	29%
Соціальний захист		
низький рівень тривоги	51,5%	19,5%
нормальний рівень тривоги	17%	51%
високий рівень тривоги	31,5%	29,5%
Загальний рівень		
низький рівень тривоги	63,5%	57,5%
нормальний рівень тривоги	26%	16,5%
високий рівень тривоги	10,5%.	26%

Таблиця 5.4.

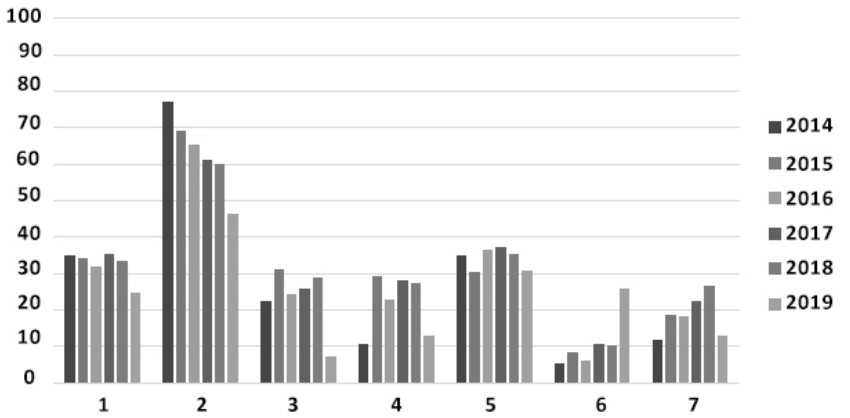
Результати дослідження середніх значень рівня особистісної тривожності

Параметр	Цивільні особи (бали)
Соціальний захист	123,52 ± 7,672
Фобічний компонент	112,82 ± 9,463
Астенічний компонент	107,83 ± 7,576
Загальний рівень	98,62 ± 8,821
Тривожна оцінка перспектив	59,73 ± 6,241
Емоційний дискомфорт	14,82 ± 0,952

Аналіз результатів дослідження, наведених у таблиці 5.4, показав, що в групи осіб, які проживали на територіях, наближених до зони збройного конфлікту, домінували такі прояви особистісної тривожності, як соціальний захист (123,52±7,672), фобічний компонент (112,82±9,463), астенічний компонент (107,83±7,576). Тобто тривожність як особистісна риса проявлялась у цих осіб найбільше при соціальних контактах, у схильності бачити соціальне середовище як основне джерело тривожного напруження та невпевненості в собі, при тому що вони заперечували фоновий стан напруженості. Також даному контингенту властиві відчуття незрозумілої загрози, невпевненості в собі, власної марності, скарги на хронічну втому, в'ялість, пасивність, розлади сну.

Спостерігається значний приріст негативних емоцій у населення, серед яких перше місце посідає почуття тривоги (рис. 5.5.), що може сприяти розвитку психопатологічних і соматичних проявів у жителів регіону збройного конфлікту.

Із рисунка 5.5. видно, що почуття страху має тенденцію до зменшення, але все ж залишається, за нашими даними, у кожного четвертого опитуваного.



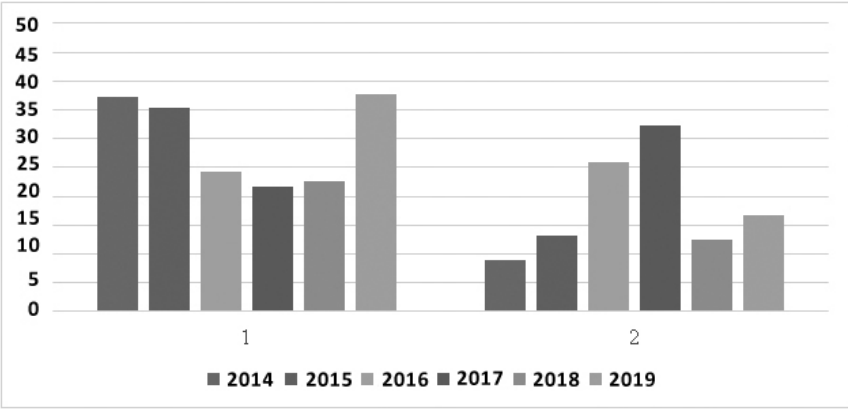
Примітка: 1 – страх, 2 – тривога, 3 – безпорадність, 4 – відчай, 5 – роздратування, 6 – байдужість, 7 – смуток

Рис. 5.5. Емоції, виявлені в населення в зоні військового конфлікту

Стани відчаю та смутку також залишаються стабільно високими. Без особливих змін у бік зменшення залишається почуття роздратування. Стан безпорадності за останній рік зменшився. Поряд із зазначеним, спостерігається тенденція до збільшення почуття байдужості.

Вивчення особливостей проявів постстресових психічних розладів у цивільних осіб, які мешкали на територіях, наближених до зони збройного конфлікту, проводилось за допомогою Міссісіпської шкали. Отримані дані наведено на рис. 5.6.

За даними дослідження 2019 року, у 16,7% осіб, які пройшли скринінг, діагностовано ПТСР, у 37,6% – відзначались окремі ознаки ПТСР, у 45,7% ознак психопатологічних порушень виявлено не було. Відбувається зростання частки осіб із окремими ознаками ПТСР до величин 2014 року (початок проведення дослідження у зв'язку з виникненням збройного конфлікту на Донбасі) та вдвічі ПТСР порівняно з 2014 роком (з 8,9% до 16,7%).



Примітка: 1 – окремі ознаки ПТСР, 2 – ПТСР

Рис. 5.6. Результати діагностики посттравматичного розладу за допомогою Міссісіпської шкали

За результатами дослідження кореляційного зв'язку було встановлено статистично значущі кореляційні зв'язки між Міссісіпською шкалою ПТСР та шкалами особистісної тривожності інтегрованого тесту тривожності. Результати дослідження представлено в таблиці 5.5.

Найбільш виражені кореляційні зв'язки було встановлено між Міссісіпською шкалою ПТСР та астенічним компонентом особистісної тривожності й емоційним дискомфортом, тобто проявами ПТСР, у більшості випадків є наявність тривожності, як індивідуально-психологічної характеристики, що провокує примноження емоційної напруги і тим самим збільшує прояви ПТСР. Скаргами таких хворих були швидка втомлюваність, в'ялість, пасивність, розлади сну, знижений емоційний фон, незадоволеність життєвою ситуацією, емоційне напруження.

Таблиця 5.5.

Результати дослідження кореляційного зв'язку між Міссісіпською шкалою ПТСР та шкалами особистісної тривожності

Параметр	Коефіцієнт кореляції
Емоційний дискомфорт	0,409**
Астенічний компонент	0,412**
Фобічний компонент	0,302**
Тривожна оцінка перспектив	0,286**
Соціальний захист	0,300**
Загальний рівень	0,279**

Примітка. Коефіцієнт кореляції rs-Спірмена: *– $p \leq 0,05$, ** – $p \leq 0,01$.

При розробці відновлювальних заходів і плануванні необхідної медико-психологічної допомоги важливим є дослідження особистісних механізмів подолання стресу і вирішення конфліктних ситуацій. Для діагностики зазначеного було обрано дослідження копінг-стратегій, що в представленій роботі проводилося за допомогою тесту копінг-стратегій Лазаруса. У таблиці 5.6 наведені отримані результати.

Результати за рівнями прояву тієї чи іншої копінг-стратегій розташувались наступним чином. Конфронтаційний копінг: норма – 44%, високий рівень – у 54,5%, дуже високий – у 1,5% респондентів. Дистанціювання: норма – 42,5%, високий рівень – 44%, дуже високий – 13,5%. Самоконтроль: норма – 27,5%, високий рівень – 50%, дуже високий – 22,5%.

Таблиця 5.6.

Дослідження копінг-стратегій у населення Донбасу

Параметр	Цивільні особи (бали)
Конфронтаційний допінг	37,42 ± 2,317
Дистанціювання	41,75 ± 2,601
Самоконтроль	49,01 ± 2,666
Пошук соціальної підтримки	52,71 ± 3,073
Прийняття відповідальності	44,95 ± 3,085
Утеча-уникнення	37,56 ± 2,301
Планування вирішення проблем	49,86 ± 3,011
Позитивна переоцінка	45,06 ± 2,598

Пошук соціальної підтримки: норма – 29%, високий рівень – 32%, дуже високий – 39%. Прийняття відповідальності: норма – 35%, високий рівень – у 38%, дуже високий – 27%. Утеча-уникнення: норма – 39,5%, високий рівень – 51,5%, дуже високий – 9%. Планування вирішення проблем: норма – 9%, високий рівень – 39,5%, дуже високий – 31,5%. Позитивна переоцінка: норма – 27,5%, високий рівень – 50%, дуже високий – 22,5%.

На основі даних, отриманих за допомогою Міссісіпської шкали, усіх обстежуваних поділили на групи: особи без ознак ПТСР, особи з окремими ознаками ПТСР, особи з ПТСР. У групі осіб із ПТСР переважаючими копінг-стратегіями були втеча-уникнення ($rs = 0{,}546$, $p \leq 0{,}05$) та дистанціювання ($rs = 0{,}433$, $p \leq 0{,}05$) (див. табл. 5.7.).

Таблиця 5.7.

Результати дослідження кореляційної зв'язку між Міссісіпською шкалою і тестом Лазаруса

Параметр	Коефіцієнт кореляції
Конфронтаційний допінг	0,344**
Дистанціювання	0,433**
Самоконтроль	0,122
Пошук соціальної підтримки	0,337**
Прийняття відповідальності	0,325**
Утеча-уникнення	0,546**
Планування вирішення проблем	0,232
Позитивна переоцінка	0,091

Примітка. Коефіцієнт кореляції rs-Спірмена: *– $p \leq 0,05$, ** – $p \leq 0,01$.

У групі осіб із ПТСР досліджувалися кореляційні зв'язки між ступенем вираженості постстресових психічних розладів й індивідуально особистісними характеристиками обстежуваних (табл. 5.8.).

Аналіз результатів дослідження кореляційних зв'язків ПТСР та індивідуально-особистісних характеристик обстежуваних показав, що в групі з високими показниками за шкалою ПТСР домінували ознаки тривожності ($rs = 0,525$, $p \leq 0,05$), депресивності ($rs = 0,434$, $p \leq 0,05$) , ворожості ($rs = 0,376$, $p \leq 0,05$).

Слід зазначити, що в зоні військового конфлікту велику роль відіграє інформаційне середовище, що певним чином впливає на психічний стан та психологічне благополуччя населення.

Таблиця 5.8.

Результати дослідження кореляційного зв'язку між проявами ПТСР та індивідуально-особистісними характеристиками

Параметр	Коефіцієнт кореляції
Соматизація	0,352**
Обсесивно-компульсивні розлади	0,360**
Міжособистісна сензитивність	0,295**
Депресія	0,434**
Тривожність	0,525**
Ворожість	0,376**
Фобічна тривожність	0,325**
Параноїльні симптоми	0,359**
Психотизм	0,322**
Загальний індекс тяжкості симптомів	0,398**
Симптоматичний дистрес	0,368**

Примітка. Коефіцієнт кореляції rs-Спірмена: *– $p \leq 0,05$, ** – $p \leq 0,01$.

Переживання людей, які перебували у військовій зоні, безслідно не минають. Ситуація, що склалася, впливає на емоційний і психічний стан населення, викликаючи паніку, агресію, страх, тривогу, почуття відчаю та приреченості. З'являються нові групи осіб, які піддаються впливу стресогенних чинників. Вони можуть входити до «групи ризику» щодо виникнення розладів психіки та поведінки, пов'язаних із стресовими факторами. Тому одним із завдань дослідження було визначити ставлення респондентів до інформаційного простору, у якому вони

знаходяться, а також оцінити якість інформації та потреби в її отриманні.

Аналіз результатів анкетування показав (рис. 5.7.), що потреба в новій інформації на початку військових дій досягала максимального значення в 77,6% обстежених, а в 2019 році ця потреба знизилася до 18,25%. Значно збільшилася кількість осіб, що не цікавляться інформацією взагалі, із 2,7% в 2014 році до 46,5% в 2019 році. При цьому відзначається неухильне зростання осіб із байдужістю та зневірою. Якщо кількість осіб, що зазнають байдужості, у 2014 році склала 5,5%, то в 2019 році їхня кількість становить 22,5%. Число осіб, які відчувають смуток, у 2014 році – 12%, у 2019 році – 26,5%.

Рис. 5.7. Результати дослідження сприйняття інформації населенням, яке мешкає в регіоні бойових дій

Аналіз результатів дослідження за допомогою опитувальника SCL-90-R показав, що в 2014 році в обстежуваних домінували тривожні переживання (2,028 ± 0,117), ознаки соматизації (1,909 ± 0,089), тобто існує дистрес, що виникає з відчуття тілесної дисфункції і виявляється в різних скаргах, болях, а також у

соматичних еквівалентах тривожності. У 2019 році домінували тривожні переживання (1,924 ± 0,104), міжособистісна сензитивність (1,830 ± 0,126), ознаки депресії (1,771 ± 0,105).

Європейська психіатрична асоціація на початку XXI століття досліджувала поширеність тривожних розладів у популяції: як часто зустрічаються тривожні розлади у людей, які перенесли психотравмуючі події. Виявилося, що депресивні розлади є у близько 10%, а тривожні розлади мають від 15-20 до 40%. Згідно зі статистикою ВОЗ близько 12% населення Центральної Європи страждають від тривожних розладів.

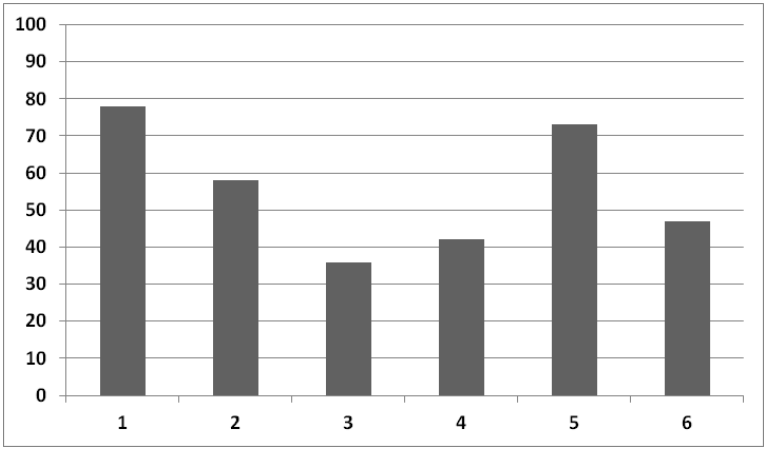
За нашими даними, у 2016 році поширеність психічних захворювань (F 40-48) склала 27,2 на 10000 населення, що на 6,7% перевищує показник 2013 року (25,5 на 10000 населення). Відзначалася тенденція зростання захворювань, пов'язаних зі стресом. Так, в 2013 році питома вага невротичних, пов'язаних зі стресом і соматоформних розладів (F40-F48) склав 18,7%, а в 2016 році 27,1%. Серед них тривожно-фобічні розлади (F40) склали 19,4% (10,4% у 2013 році); панічний розлад (F41) 1% (не виявлено в 2013 році); генералізований тривожний розлад (F41.1) 34,0% (30,0% у 2013 році); обсесивно-компульсивний розлад (F42) 1,8% (1,5% у 2013 році); реакція на важкий стрес і порушення адаптації (F43) 24,3% (20,9% у 2013 році); диссоціативні (конверсійні) розлади (F44) 1% (10,4% у 2013 році); соматоформні розлади (F45) 6,8% (6,0% у 2013 році).

У роботі з дітьми й підлітками було також сформовано психодіагностичний комплекс та перевірено ефективність його використання. При обстежені психологічного стану дітей 5-7 років використовувалися методи діагностики емоційно-вольової сфери. Для встановлення відхилень у психічному здоров'ї дитини використовувалися проєктивні та стандартизовані методики: методика «Паровозик» (С.В.Веліїва), опитувальник страхів (А.І. Захаров); «Кактус» (М.О. Панфілова), «Неіснуюча тварина» (М.З. Друкаревич), «Малюнок сім'ї» (Г.Т. Хоментаускас); анкета з визначення тривожності та агресивності у дітей (Г.П. Лаврент'євої та Т.М.Тітаренко). За результатами діагностики було встановлено наявність тривожності, агресії, страхів,

скритності, самотності, визначено рівень самооцінки, що буде розглянуто більш детально далі.

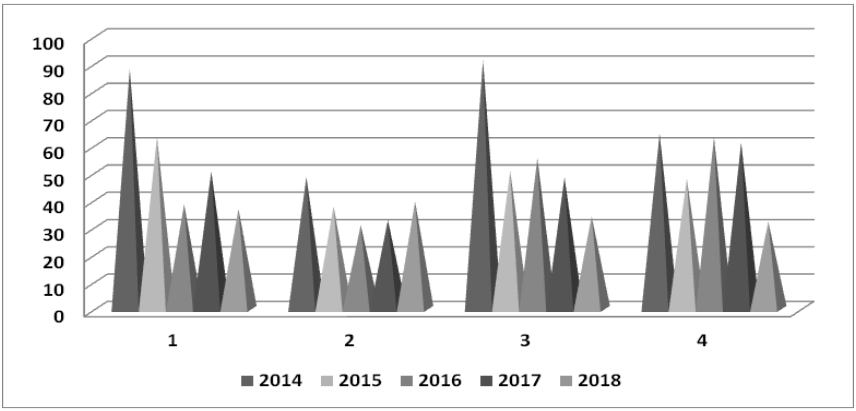
До складу психодіагностичного комплексу, що дозволяє виявити пограничні та клінічні особливості емоційно-вольової сфери підлітків, уходили стандартизовані та проєктивні методи: опитувальник темпераменту Г. Айзенку, «Дитячий опитувальник неврозів» (Седнев В.В., Збарський З.Г., Бурцев О.К.), опитувальник А. Басса-А.Дарки для визначення характеру та рівня агресії, метафоричні асоціативні карти (набір COPE), проєктивна методика «Намалюй свій страх».

На прикладі результатів медико-психологічного дослідження емоційної сфери та соматичного стану дітей, які знаходяться в зоні проведення антитерористичної операції, наочно продемонстровані порушення стану здоров'я внаслідок стресового впливу (рис. 5.8.). Окрема динаміка страхів у дітей 5-7 років та 10-14 років представлена на рисунках 5.9. та 5.10. відповідно.



Примітка: 1 – тривога, 2 – вегетативні розлади, 3 – астенія, 4 – порушення сну, 5 – страх війни, 6 – соціальні страхи

Рис 5.8. Розлади емоційної сфери дітей у ситуації стресового впливу



Примітка: 1– страх війни; 2 – страх фізичної шкоди; 3 – страх темряви; 4 – медичні страхи

Рис 5.9. Динаміка страхів у дітей 5-7 років (2014-2018 роки)

Із рисунку 5.9. видно наявність страху війни протягом усього періоду проведення досліджень. Слід наголосити на тому, що для дітей дошкільного віку, ураховуючи їхній психологічний розвиток, страх війни є невластивим для даної вікової категорії осіб, тобто – набутим за умов соціально-психологічного напруження, що вперше був виявлений у 2014 році під час громадянського конфлікту на Сході України.

Було встановлено збільшення рівня агресії серед дітей у групі респондентів зі страхом війни (p=0,05). Це підтвердило одне з припущень, що діти, які бояться війни, більш агресивні, ніж діти з відсутністю цього страху. Така форма поведінки виникає внаслідок емоційної травми, що проявляється в дитині поведінковими і вербальними відхиленнями. Переважання страху війни в дітей даної категорії зумовлено специфічними умовами життєдіяльності в умовах психотравмуючої ситуації.

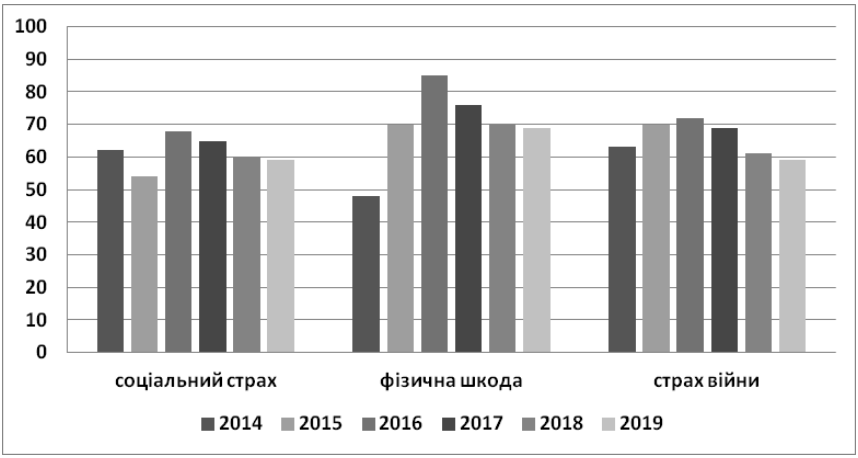
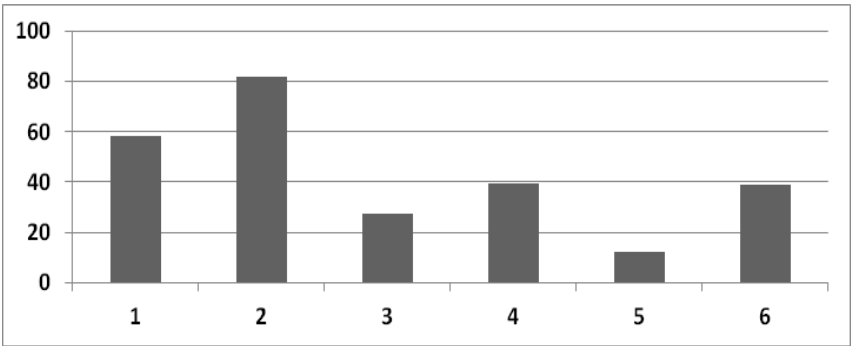


Рис 5.10. Динаміка страхів у дітей 10-14 років

Підвищені показники за соціально-значимими шкалами «Соціальний страх» та «Страх фізичної шкоди» підтверджують відчуття небезпеки з боку соціуму. Очікування небезпеки і відчуття тривоги при взаємодії з іншими людьми сприяє розвитку соціального страху. Формування цього виду страху найбільш часто відбувається в дитячому та підлітковому віці. Саме тоді особистість найбільш вразлива, схильна до впливу та формування негативного соціального досвіду. Тривале перебування дитини в стресових обставинах здатне значним чином вплинути на сприйняття та формування картини світу загрозливого майбутнього. Таким чином, дитина ізольована від суспільства та соціально неадаптована.

При медичному дослідженні групи дітей відзначились порушення з боку серцево-судинної системи (рис 5.11.).



Примітка: 1 – болі в серці; 2 – порушення серцевого ритму; 3 – задишка; 4 – відчуття нестачі повітря; 5 – підвищення артеріального тиску; 6 – зниження артеріального тиску.

Рис. 5.11. Порушення серцево-судинної системи дітей у ситуації стресового впливу

Визначено зв'язок між показниками «Тривога» та «Порушення серцевого ритму». Дана особливість говорить про негативний вплив занепокоєння на роботу серця ($r=0,912$; $p<0,05$). Таким чином, із початком військових дій, що мають усі ознаки гібридних, чітко простежується тенденція до зростання як донозологічних, так і клінічно окреслених форм психічної патології.

Структура патології кардіологічного прийому представлено на рисунку 5.12.

За представлений період прослідковується зростання частки патології серцевого ритму в структурі з 28,1% до 47,2%, що пояснюється впливом емоційного стану дітей та підлітків, які мешкають у зоні ООС (АТО).

Рис. 5.12. Структура патології кардіологічного прийому

Ураховуючи взаємозалежність психологічного комфорту та соматичного стану, були проаналізовані скарги з боку серцево-судинної системи (рис. 5.13.)

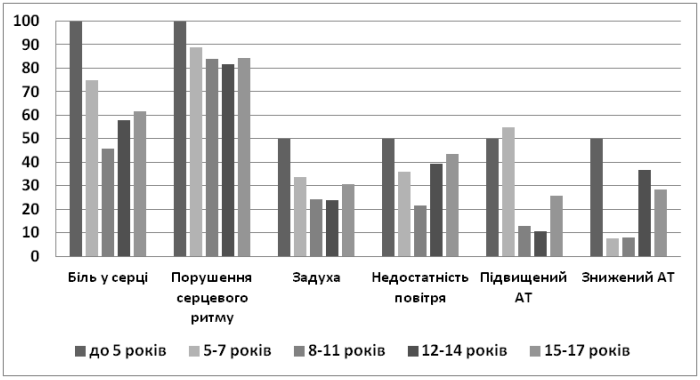


Рис. 5.13. Стан серцево-судинної системи при емоційно-вольових порушеннях у дітей (у стані тривоги)

За результатами досліджень і проведеного статистичного аналізу встановлено лінійну залежність між емоційно-вольовими порушеннями та скаргами з боку серцево-судинної системи. Скарги часто мали психосоматичний характер (задуха, біль у серці, порушення серцевого ритму, підвищення або зниження АТ), що потребують медико-психологічної реабілітації та лікування.

Отриманні результати дослідження дорослих і дітей свідчать про необхідність комплексних заходів щодо відновлення психосоматичного здоров'я. Ґрунтуючись на клінічному досвіді ДЗ «НПМ РДЦ МОЗ України», створено комплексну модель реабілітації та абілітації, в основу якої покладено медикаментозне лікування, фізіотерапевтичне лікування, психотерапія (рис. 5.14.). При проведенні лікувально-корекційних заходів для осіб із тривожними розладами ефективно застосовується когнітивно-поведінкова терапія, що включає в себе вироблення адекватного сприйняття й копінг-реакції, які переводять тривогу з циклічного процесу в лінійний процес, що сприятиме поступовому згасанню тривоги й редукції розладу.

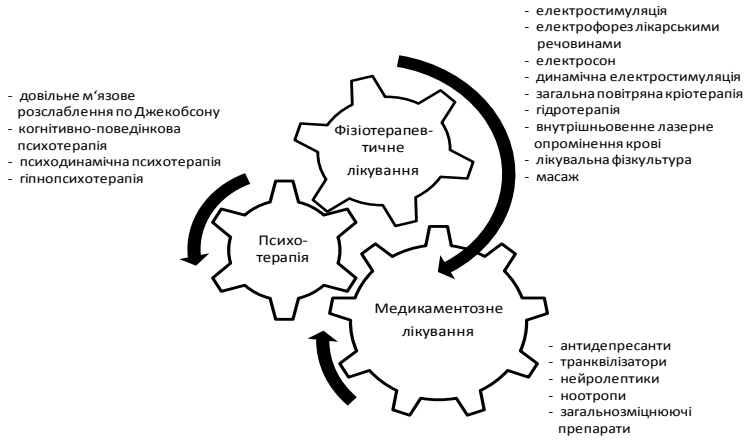


Рис. 5.14. Комплексна медико-психологічна реабілітація та абілітація

Слід підкреслити, реалізація комплексного застосування реабілітаційних заходів здійснюється в амбулаторних умовах, що дає високі показники лікувального (компетентна індивідуалізація кожного окремого випадку й чітка маршрутизація пацієнтів підвищує показники прискореного відновлення, широкі можливості реалізації новітніх лікувально-реабілітаційних технологій), економічного (зменшення кількості днів перебування на лікарняному, курсу лікування в межах лікарні, зменшення витрат державного бюджету на соціальні виплати) і соціального (хворі мобільні, не мають заборони щодо переміщення, радикально не змінюючи звичайного способу життя) ефектів для держави. Таким чином, організація реабілітаційної допомоги потребує державного регулювання, щоб це було не фрагментарною допомогою особам, які її потребують, а структурованою й регламентованою системою.

5.3. Реабілітація як складова державної політики у сфері інформаційно-психологічної безпеки

Розвиток системи ефективної реабілітації із врахуванням сьогоденних викликів, без сумніву, можна віднести до найбільш важливих задач не тільки у сфері охорони здоров'я, але й державної політики взагалі. Як бачимо, стан речей, численні наукові дослідження та організаційно-правові заходи не лише не вичерпали проблему, а й, навпаки, засвідчили її глибину та багатовекторність. Нові ризики, пов'язані з інформаційно-психологічною безпекою, у тому числі й бойові дії на Сході України, підкреслюють необхідність постійного розвитку теоретичного фундаменту, у межах якого формуються науково обґрунтовані принципи побудови та практичної організації реабілітаційного процесу.

Результати власних досліджень та інші наукові роботи [20-27] доводять, що порушення інформаційно-психологічної безпеки у вигляді збитку психічному стану людини (інформаційно-психологічна турбулентність, тривога, страх, ПТСР) потре-

бують постфактумного реагування у вигляді, насамперед, медико-психологічної допомоги з акцентом на вирішення психологічних проблем. Так, за офіційними даними (2017 рік), тільки серед демобілізованих військовослужбовців ЗСУ, які звернулися до закладів охорони здоров'я, 54% потребують медичної, до 30% – фізичної і понад 80% – психологічної реабілітації. У 2019 році тільки 2% тих, хто її потребує, отримали реабілітаційну допомогу. Дослідниками відзначається взаємозв'язок успішності реабілітації в післяекстремальний період з індивідуально-психологічними особливостями людини. Вивчення цих особливостей є актуальною темою у вирішенні проблеми збереження психологічної цілісності особистості, самоактуалізації, вибору адекватних копінг-стратегій у післяекстремальних умовах. Не менш важливим є сприятлива психічна адаптація особистості. Александровський Ю.А. [28] до провідних підсистем в ієрархії психічної адаптації відносить наступні:

– пошук, сприйняття й переробка інформації (основа пізнавальної діяльності);

– емоційне реагування, що створює, зокрема, «особистісне» ставлення до одержуваної інформації та є «найбільш інтегрованою» формою активності;

– соціально-психологічні контакти;

– бадьорість і сон;

– ендокринно-гуморальна регуляція.

Як видно, на перших місцях стоять інформаційна, емоційна та соціально-психологічна складові, що дають логічну підставу для виділення зі складу національної безпеки інформаційно-психологічної безпеки. Остання сприяє психологічному благополуччю особистості, мінімізує різноманітні ризики інформаційного середовища, тим самим формує адекватне відношення до навколишнього світу, сучасного інформаційного поля й самої себе. Організація інформаційно-психологічної безпеки на державному рівні виступає складовою збереження психічного здоров'я.

Психічне здоров'я в сучасному розумінні – це не тільки відсутність виражених психічних розладів у індивідуума, але й стан рівноваги та гармонії із навколишнім світом, суспільством, наявність душевних, психічних резервів для подолання стресів і труднощів, які виникають [29]. Психічне здоров'я є об'єктивним критерієм благополуччя особистості, а психологічне благополуччя – суб'єктивним (відчуттям щастя та задоволеності життям в цілому).

Із визначень випливають дві важливі для розгляду гіпотези: 1) превенцією ризиків завдання психічних збитків є *абілітація*; 2) у разі настання психічних збитків постфактумним їх усуненням є *реабілітація*.

Останнє поняття є більш дослідженим, ніж попереднє, але й не тільки сам термін, але й суть реабілітації у різних країнах трактують неоднаково.

Так, в англійському варіанті термін «rehabilitation» означає реабілітацію, відновлення здоров'я та працевлаштування, відновлення працездатності. У франкомовних країнах уважають за краще говорити про «реадаптацію» – пристосування до трудової діяльності. Але в будь-якому випадку мова ведеться в контексті медичної реабілітації. За визначенням ВООЗ (1980), медична реабілітація – це активний процес, метою якого є досягнення повного відновлення порушених унаслідок захворювання або травми функцій, або, якщо це нереально, – оптимальна реалізація фізичного, психічного й соціального потенціалу інваліда, найбільш адекватна інтеграція його в суспільство. Це визначення розширює поняття від «пристосування до трудової діяльності» до «відновлення порушених функцій», але акцентується на інвалідах. Також у Великому тлумачному словнику української мови [30] подається таке визначення медичної реабілітації: «комплекс медичних, педагогічних, професійних засобів, спрямованих на відновлення (або компенсацію) порушених функцій організму й працездатності хворих та інвалідів», яке теж можна вважати недосконалим. З огляду на визначення психічного здо-

ров'я, мета реабілітації повинна полягати не тільки у відновленні працездатності чи порушених функцій, а й у відновленні психологічної цілісності, гідності людини (а не інваліда), її соціально-громадської самостійності, самоактуалізації. Спираючись на це, а також враховуючи вищезгадану теорію Александровського Ю.А., акцент необхідно зосередити на психологічній реабілітації як першочерговій порівняно з іншими. Подібні погляди щодо реабілітації можна все частіше зустріти в роботах вітчизняних дослідників та законодавчих актах. Наприклад, Лянной Ю.О. визначає реабілітацію як «складний багатофакторний процес, який ураховує різноманітні, тісно пов'язані і взаємодоповнюючі види, серед яких виділяють медичну, фізичну, психологічну, соціальну, професійну, економічну, педагогічну, спортивну, побутову, технічну, оздоровчу та правову реабілітацію» [31]. Проєкт закону «Про систему реабілітації в Україні» дає таке визначення: «сукупність заходів, що допомагають особам, які мають або в яких можуть виникнути обмеження життєдіяльності, досягнути та підтримувати оптимальний рівень функціонування у взаємодії з навколишнім середовищем, соціальну інтеграцію та незалежність» [32]. Новаторський підхід у цьому проєкті нами бачиться в поділі реабілітації на такі види: фізико-медичну, психологічну, професійну, рекреаційно-спортивну. Але поряд із цим у проєкті є ряд недоліків.

По-перше, абілітація визначена як «сукупність заходів реабілітації, що допомагають особам зі вродженим обмеженням життєдіяльності або таким, що виник у ранньому віці, досягнути максимального рівня функціонування при взаємодії із навколишнім середовищем». При всій повазі до авторів проєкту, абілітація не тотожна реабілітації, хоча вони й знаходяться в одній площині системи підтримки і відновлення благополуччя особистості. Та й надалі для визначення абілітації взято архаїчне формулювання в дуже вузькому розумінні.

По-друге, указано, що психологічна реабілітація може бути представлена як самостійна програма, так і входити до ін-

дивідуальної програми реабілітації спільно з медико-фізичною реабілітацією. А хіба вона не може входити до програми реабілітації спільно з професійною та рекреаційно-спортивною?

По-третє, психологічна реабілітація викладена в двох тлумаченнях – короткому й розширеному. Коротке: це «сукупність заходів реабілітації, спрямованих на відновлення або компенсацію порушених психічних функцій, станів, якостей, властивостей, особистого й соціального статусу особи, її психологічна адаптація до зміненої життєвої ситуації та формування в неї свідомої активної участі в реабілітаційному процесі». Це визначення в цілому відображає суть психологічної реабілітації, за виключенням останньої фрази («формування в неї свідомої активної участі в реабілітаційному процесі»), яку запозичили, на наш погляд, із класичного визначення медичної реабілітації, де психологічна є лише складовою. Розширене ж визначення (Стаття 23) є суцільним нагромадженням виразів, яке важко систематизувати.

Найбільш креативним можна вважати визначення, викладене в діючому законодавчому акті – Постанові Кабінету Міністрів від 27 грудня 2017 р. №1057 [33]: «психологічна реабілітація – комплекс заходів, що здійснюються з метою збереження, відновлення або компенсації порушених психічних функцій, якостей, особистого та соціального статусу особи, сприяння психосоціальній адаптації до зміненої життєвої ситуації, осмислення досвіду, отриманого в екстремальній ситуації, та застосування його в житті».

Щодо абілітації, то не тільки зазначений проєкт Закону, але й багато дослідників дають звужене або неоднозначне трактування, часто отожнюючи реабілітацію й абілітацію. Так, Л.О. Бадалян дає таке визначення: «Абілітація передбачає лікувально-педагогічну корекцію рухової, психічної та мовної сфери дітей молодшого віку; реабілітація передбачає такі заходи щодо дітей старшого віку та дорослих» [34]. На думку Л.І.Боровікова, «абілітація – це не компенсація і, тим більше, не реабілітація.

Це саме робота з формування соціально-психологічних і духовно-моральних новоутворень, що забезпечують зростання якості життя дітей-інвалідів» [35]. Більш розширене формулювання абілітації, спираючись на роботи інших дослідників [36, 37], можна представити так: «це лікувальні, педагогічні, психологічні або соціальні заходи по відношенню до інвалідів або морально підірваних людей, спрямовані на адаптацію їх до життя в суспільстві, на придбання можливості вчитися та працювати».

У попередніх власних роботах визначено абілітацію як «комплекс психофізіологічних, фізіологічних, біологічних, психологічних заходів, спрямованих на відновлення фізіологічних функцій або недорозвинених здібностей людини шляхом компенсаційного лікування й соціально-психологічних заходів, необхідних для створення можливостей формування, розвитку та реалізації особистості, забезпечення функціональної свободи дій, поліпшення фізичних і психічних якостей та адаптації до життєдіяльності» [22].

Таке визначення має право на існування, але, з огляду на поняття інформаційно-психологічної безпеки в нашому контексті, а також висунуті гіпотези, метою як абілітації, так і реабілітації є психологічне благополуччя. Для розкриття теми саме з такого ракурсу, ми залучили підходи спеціальної (корекційної) психології. Як відомо, предметом вивчення спеціальної психології є розвиток психіки, що протікає за несприятливих умов.

У категоріях спеціальної психології *реабілітація* – система медико-психологічних, педагогічних і соціальних заходів, спрямованих на відновлення, корекцію або компенсацію порушених психічних функцій, станів, особистісного та соціально-трудового статусу хворих, інвалідів, осіб, які перенесли захворювання; абілітація – система заходів, спрямованих на формування ефективних способів соціальної адаптації у можливих для людини межах [38].

У наведених визначеннях можна побачити інші поняття: «компенсація» та «адаптація».

Компенсація – відшкодування, вирівнювання, розвиток порушених або недорозвинених функцій, перебудова збережених функцій для заміщення порушених; придбання в навчанні і вихованні способів діяльності та поведінки, що сприяють соціальній адаптації та інтеграції [38]. Знову бачимо застосування поняття «адаптація», звідки можна зробити висновок, що існує системний зв'язок між адаптацією та попередніми поняттями.

Адаптація – особливий процес відновлення порушеної рівноваги між індивідом і середовищем шляхом внутрішніх змін самого індивіда [38]. Це коротке визначення потребує більш детального аналізу. Узагалі, визначаючи суть поняття «адаптація», дослідники виходять із того, що воно може розглядатися як процес, стан, властивість або результат діяльності, який виникає за певних умов, триває протягом певного періоду, поки не буде встановлено динамічну рівновагу між системами, які адаптуються [39]. Ж. Піаже [40] вперше розглянув адаптацію як двостороннє явище в єдності процесів активної зміни особистістю навколишнього середовища та зміни власного внутрішнього світу. У процесі адаптації людина мимоволі використовує певні стратегії, серед яких, можна виділити кілька векторів: фізіологічний, психологічний, соціальний. У сукупності вони розглядаються багатьма дослідниками як багаторівнева структурно-функціональна система – психічна адаптація [41, 42]. Одну з точок зору (Александровський Ю.А.) було представлено вище.

Виходячи з розглянутих передумов, пропонуємо модель цілісного забезпечення інформаційно-психологічної безпеки (рис. 5.15.), що передбачає як захист, так і відновлення психологічного благополуччя особистості.

Як видно з рисунку, базовими в досягненні інформаційно-психологічної безпеки є такі процеси: реабілітація, абілітація, компенсація та адаптація.

Рис. 5.15. Модель забезпечення інформаційно-психологічної безпеки (за Панченком О.А., 2019)

Усі вони, триваючи в часі, здійснюються на чотирьох рівнях своєї організації: біологічному, психологічному, соціальному, соціально-психологічному. Кожен із рівнів має певний алгоритм реалізації:

1. Біологічний – внутрішні резерви.
2. Психологічний – механізми психологічного захисту.
3. Соціально-психологічний – копінг-технології.
4. Соціальний – інтеграція (соціалізація).

Кожен із рівнів має інформаційний супровід (паралельний інформаційний рівень). Важливо відзначити, що перераховані рівні і властиві їм алгоритми не мають суворих меж поділу та функціонування.

Абілітація, як і реабілітація, є зовнішнім процесом. Відмінність у тому, що ключовим словом при абілітації є «формування». Ми додали б ще й «прищеплення», «придбання». Оскільки реалізація цього процесу, як і всіх інших, відбувається на чотирьох різних рівнях, поняття абілітації або локалізується в прив'язці до даного рівня, або «проводиться» певний контингент (наприклад, діти-інваліди) від одного рівня до іншого. Цікаво, що визначення абілітації в прив'язці до інформаційного рівня ми не знаходимо в доступних джерелах інформації. Узявши до уваги викладений матеріал і наші попередні роботи [3], подаємо наступне визначення: «Інформаційно-психологічна абілітація – це адаптивно розвивальна діяльність із формування / прищеплювання /придбання навичок турбулентного мислення в умовах інтенсивних ризикових інформаційних факторів із метою підтримки психологічного благополуччя з відповідним забезпеченням якості життя людини».

У поняття «турбулентність мислення / турбулентне мислення» ми вкладаємо специфічне явище, що відбувається в розумовому процесі, засноване на неформальному, евристичному підході до аналізу ситуації та прийняття рішень (досвід, креативність, інтуїція, спритність, винахідливість і т.д.). Таке мислення формується шляхом як цілеспрямованих дій з боку держави й суспільства, так і занять із самовдосконалення особистості.

Приведені визначення абілітації розширюють теоретичне підґрунтя для практичної можливості її застосування поряд із реабілітацією і повинні бути враховані в законотворчій діяльності.

Отже, запропонована модель забезпечення інформаційно-психологічної безпеки системно поєднує поняття реабіліта-

ція-абілітація-компенсація-адаптація та відображає чотири рівні їхньої організації (біологічний, психологічний, соціальний, соціально-психологічний), кожен із яких супроводжується складовою інформаційного рівня.

Державна політика у сфері інформаційно-психологічної безпеки повинна полягати в прискоренні створення дієвої системи психологічної реабілітації та абілітації, де нові нормативно-правові засади, що ґрунтуються на сучасних наукових доробках, є першочерговими.

Список використаних джерел

1. Федорова О.Н. Информационно-психологическая безопасность личности в информационном обществе. Вестник Дальневосточного государственного технического университета. 2011. № 2 (7). С. 21-34.

2. Скрипаченко Т.В. Психологічні особливості інформаційного стресу. Проблеми сучасної психології: збірник наукових праць. 2018. № 1(13). С. 153-158.

3. Ткачишина О.Р. Психологічна безпека у контексті маніпулятивного впливу на свідомість особистості. Теорія і практика сучасної психології. 2019. № 1. Т. 1. С. 178-182.

4. Спилбергер Ч. Д. Концептуальные и методологические проблемы исследования тревоги. Стресс и тревога в спорте. М. 1983. С. 1224.

5. Маслова Т.М., Покацкая А.В. Тревожность личности как фактор развития стрессоустойчивости. Азимут научных исследований: педагогика и психология. 2019. Т. 8. № 2 (27). С. 352-354.

6. Соловьева С.Л. Тревога и тревожность: теория и практика. Медицинская психология в России. 2012. №6 (17). URL: http://medpsy.ru (дата звернення: 05.05.2020).

7. Панченко О.А., Банчук Н.В. Информационная безопасность личности. 1-е изд. Донецк: ФОП Дмитренко. 2010. 736 с.

8. Малкова Е.Е. Тревога как ресурс адаптивного развития личности. Вестник СПбГУ. Сер. 16. 2014. Вып. 2. С. 34-40.

9. Прихожан А.М. Тревожность у детей и подростков: психологическая природа и возрастная динамика. М.: Московский психолого-социальный институт; Воронеж: МОДЭК. 2000. 304с.

10. Кузнецова Ю.М., Чудова Н.В. Психология жителей Интернета. М.: Изд-во ЛКИ. 2008. 224 с.

11. Франкл В. Человек в поисках смысла: сборник: пер. с англ. и нем. Общ. ред. Л.Я. Гозмана и Д.А. Леонтьева. М.: Прогресс 1990. 368 с.

12. Панченко О.А. Турбулентное мышление в условиях тревожного предчувствия. Реалізація тривоги у психічні та соматичні розлади у населення в зоні проведення антитерористичної операції: збірник тез доповідей учасників науково-практичної конференції з міжнародною участю За заг. ред. д. мед. н., проф., Заслуженого лікаря України. «Контраст» 2018. С. 7-14.

13. Ханин Ю.Л. Краткое руководство к применению шкалы личностной и реактивной тревожности. Л. 1976. 127с.

14. Черненко І.І., Чухно І.А. Сучасні методи психологічної терапії хворих із посттравматичними стресовими розладами в контексті їх медико-соціального значення. Новости медицины и фармации. 2017. №5 (91). URL: http://www.mif-ua.com/archive/article/45078. (дата звернення: 05.05.2020).

15. Юрьева Л.Н. Тревога: диагностика, терапия и профилактика. Нейро news психоневрология и нейропсихиатрия. 2010. №3 (22). С.50-54.

16. Ткач М.И. Оказание психологической помощи населению Донбасса в период вооруженного конфликта и в восстановительный период. Проблемы психологических последствий, связанных с радиационными авариями и другими чрезвычайными ситуациями: материалы международной научно-практической конференции. Квадратон. 2015. С. 23- 25.

17. Панченко О.А., Кутько И.И., Зайцева Н.А. Социально-стрессовые расстройства: мирное население в эпицентре

военных действий. Новости медицины и фармации. № 15 (509). 2014. С. 6.

18. Ястребов В.С., Митихина И.А., Митихин Г.Т. и др. Психическое здоровье населения мира: социально-экономический аспект (по данным зарубежных исследований 2000-2010 гг.). Журнал неврологии и психиатрии им. С.С. Корсакова. 2012. №2. С. 4-13.

19. Тарабрина Н.В. Психология посттравматического стресса. Изд-во Института психологии РАН. 2009. 304 с.

20. Панченко О.А. Реабилитация участников ликвидации последствий аварии на Чернобыльской АЭС с пограничными психическими расстройствами. Лікарська справа. 1994. № 5-6. С. 84-86.

21. Вальчук Э.А. Диспансеризация и медицинская реабилитация. Вопросы организации и информатизации здравоохранения. 2009. N 2. С. 16-21.

22. Волошок О.В. Психологічний аналіз проблеми тривожності особистості. Проблеми сучасної психології. 2010. Вип. 10. С. 120-128.

23. Панченко О.А. Информационно-психологическая безопасность в условиях гражданского противостояния. Актуальні дослідження в сучасній вітчизняній екстремальній та кризовій психології: монографія. За заг. ред. В.П. Садкового, О.В. Тімченка; НУЦЗУ. Х: ФОП Мезіна В.В. 2017. С.124-139.

24. Панченко О.А. Психологическая турбулентность в условиях информационной войны. 2018. URL: http://www.psyh.kiev.ua/Панченко_О.А._Психологическая_турбулентность_в_условиях_информационной_войны (дата звернення: 10.03.2020).

25. Сафін О.Д. Основні підходи до функціонування системи психологічної реабілітації учасників антитерористичної операції. Актуальні дослідження в сучасній вітчизняній екстремальній та кризовій психології: монографія. За заг. ред. В.П. Садкового, О.В. Тімченка. НУЦЗУ. Х: ФОП Мезіна В.В. 2017. С.369-382.

26. Мась Н.М. Особливості психологічної реабілітації учасників антитерористичної операції. Актуальні дослідження в сучасній вітчизняній екстремальній та кризовій психології: монографія. За заг. ред. В.П. Садкового, О.В. Тімченка; НУЦЗУ. Х: ФОП Мезіна В.В. 2017. С.383-402.

27. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавничий дім «АртЕк». 2018. 446 с.

28. Александровский Ю.А. Предболезненные состояния и пограничные психические расстройства (этиология, патогенез, специфические и неспецифические симптомы, терапия). М.: Литтерра. 2010. 272 с.

29. Панченко О.А., Банчук Н.В. Информационная безопасность личности: монография. Киев: КИТ. 2011. 672с.

30. Великий тлумачний словник сучасної української мови (з дод. і допов.) уклад. і голов. ред. В. Т. Бусел. К.; Ірпінь. ВТФ «Перун». 2005. 1728 с.

31. Лянной Ю.О. Визначення видів реабілітації у професійній підготовці майбутніх магістрів з фізичної реабілітації. Вісник Чернігівського національного педагогічного університету. Сер.: Педагогічні науки. Фізичне виховання та спорт. 2013. Вип. 112 (2). С. 177-182.

32. Про систему реабілітації в Україні: проєкт Закону України. URL: https://novynarnia.com/2017/10/02/zakon-ukrayini-pro-sistemu-reabilitatsiyi-v-ukrayini-proekt (дата звернення: 06.05.2020).

33. Про затвердження Порядку проведення психологічної реабілітації постраждалих учасників Революції Гідності, учасників антитерористичної операції та осіб, які здійснювали заходи із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях: Постанова Кабінету міністрів України від 27 грудня 2017 р. №1057. URL: https://zakon.rada.gov.ua/laws/show/1057-2017-%D0%BF (дата звернення: 06.05.2020).

34. Бадалян Л.О. Невропатология: Учебник. 2-е изд. М.: Изд-во «Академия». 2003. 368 с.

35. Этюды абилитационной педагогики: из опыта работы «Школы Бороздина». Монографическое эссе. Под ред. Л.И. Боровикова. Новосибирск: Изд-во НИПК и ПРО. 2000. 145 с.

36. Чепурышкин И.П. К вопросу о сущности понятия «абилитация» как педагогический феномен. Личность, семья и общество: вопросы педагогики и психологии: сб. ст. по матер. I междунар. науч.-практ. конф. № 1. Часть IV. Новосибирск: СибАК, 2010. URL:http://sibac.info/conf/pedagog/i/35394 (дата звернення: 06.05.2020).

37. Беляева И.А., Бомбардирова Е.П., Токовая Е.И., Харитонова Н.А., Лазуренко С.Б., Турти Т.В., Илларионова М.С. Немедикаментозная абилитация детей с перинатальными поражениями нервной системы. Вопросы современной педиатрии. 2017. 16 (5). С. 383-391.

38. Лемех Е.А. Основы специальной психологии: лекции. URL: http://elib.bspu.by/handle/doc/3374 (дата звернення: 07.05.2020).

39. Хаустова А. И. Социально-психологическая адаптация. Молодой учёный. № 26 (130). 2016 г. С. 614-616.

40. Пиаже, Ж. Избранные психологические труды. М.: Международная педагогическая академия. 1994. 680 с.

41. Березин Ф.Б. Психическая и психофизиологическая адаптация человека. Л.: Наука. 1988. 270 с.

42. Меерсон Ф.З. Адаптация, стресс и профилактика. М.: Наука. 1981. 278 с.

РОЗДІЛ 6

Законодавчі засади та правове забезпечення інформаційної безпеки

6.1. Система забезпечення інформаційної безпеки держави

Сучасні турбулентні виклики для держави, зумовлені впливом комплексу соціально-демографічних, економічних, політичних, правових, інформаційних, психологічних і технологічних факторів, вимагають системного реагування, адекватної трансформації сектору безпеки.

Сьогоднішній стан законодавчої основи забезпечення національної безпеки та інформаційної безпеки, як її складової, можна визначити як стан системи, що знаходиться в стадії формування, а тому неминуче несе якості перехідного етапу.

У сучасних реаліях України в умовах реформування всіх сфер її життєдіяльності, у тому числі й інформаційній, проблема інформаційної безпеки і створення механізмів її забезпечення є однією із ключових.

Практично щодня у світі й державі відбуваються різноманітні події, висвітленням яких займаються засоби масової інформації. Від того, наскільки об'єктивною й достовірною буде інформація, що надається, залежить те, який інформаційний вплив вона матиме на одержувачів і як вони на неї реагуватимуть. Держава, суспільство – явища складні, і для їх нормальної взаємодії дуже важливий обмін інформацією, що стосується політичних, економічних, соціальних, культурних та інших сфер її життєдіяльності. Від своєчасності передачі, отримання інформації залежить, наскільки швидко розвиватиметься держава, суспільство. Функція забезпечення інформаційного розвитку суспільства та інформаційної безпеки здійснюється всім державним механізмом, доказом чого служить те, що активно

реалізується в Україні і світі концепція «електронної держави», суть якої полягає в активному використанні всіма державними органами у своїй повсякденній діяльності інформаційних технологій. Така відкритість діяльності держави підвищує довіру суспільства до неї. Відповідно, функція забезпечення інформаційного розвитку суспільства й інформаційної безпеки сприяє розвитку науки і вдосконаленню практики, а також є найважливішим засобом усунення наслідків соціальних негараздів.

Наука, у свою чергу, не тільки збільшує рівень знань з означеної проблеми, а й виробляє необхідні підходи щодо консолідації правового простору, удосконалення правових засобів задля захисту суверенітету держави, дотримання національних інтересів та запобігання загрозам національній безпеці держави.

Із огляду на сказане, представляє інтерес наукове визначення поняття «система забезпечення інформаційної безпеки» (СЗІБ), яке має не лише суто теоретичне, а й практичне значення, пов'язане із необхідністю формування системи органів державного управління інформаційною безпекою держави.

В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський розглядають СЗІБ як систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення [1]. Як бачимо, автори в громіздкому визначенні поєднують суб'єктивний та нормативний підходи, не вказуючи елементів системи. Інший підхід демонструє А.А. Стрельцов, включаючи до СЗІБ такі елементи: суб'єкти інформаційних процесів, інформація, призначена для використання суб'єктами інформаційного суспільства, інформаційна інфраструктура, суспільні відносини, які складаються у зв'язку зі створенням, зберіганням, передачею та розповсюдженням інформації [2]. Але вчений, на наш погляд, розглядає механізм забезпечення інформаційної безпеки, а не

саму систему. Очевидним є те, що СЗІБ є сукупністю окремих елементів, якими, зазвичай, є об'єкт, суб'єкти та види. У той же час окремими її складовими є основні характеристики, рівні інформаційної безпеки та перелік загроз.

Суттєвим є висловлювання В.А. Ліпкана, що функціонування СЗІБ не обмежується лише великим масивом нормативно-правових актів. Не можна констатувати остаточне створення основних елементів системи забезпечення інформаційної безпеки. Це й несформованість системи забезпечення національної безпеки, і невизначеність політики національної, а отже, й інформаційної. Урешті-решт, недосконалість нормативно-правового регулювання даних процесів негативно впливає і на державне управління в даній сфері [3].

Забезпечення інформаційної безпеки держави – це достатньо нова державна функція з ще не представленими об'єктами та вміщенням методів та інструментів. Її формування обумовлене необхідністю захисту суспільства та держави від інформаційних загроз, пов'язаних із розвитком новітніх інформаційно-комунікаційних технологій. Масштаби негативних наслідків цих загроз для держави, організацій, людей уже усвідомлені світовим суспільством, тому важливим завданням держави є розробка системи заходів задля їх попередження та нейтралізації. Базовими складовими СЗІБ виступають формування концепції, визначення принципів і функцій цієї системи (рис. 6.1.).

Основні принципи інформаційної безпеки були викладені в першому розділі монографії, але слід доповнити, що для забезпечення більш дієвої організації інформаційної безпеки необхідно враховувати також формування взаємної дієвості суб'єктів і об'єктів у сфері державного управління інформаційною безпекою; регламентацію заходів, пов'язаних із попередженням або зниженням руйнівного впливу можливих загроз і негативних випадків у інформаційно-технологічному суспільстві та світовий досвід інформаційної безпеки.

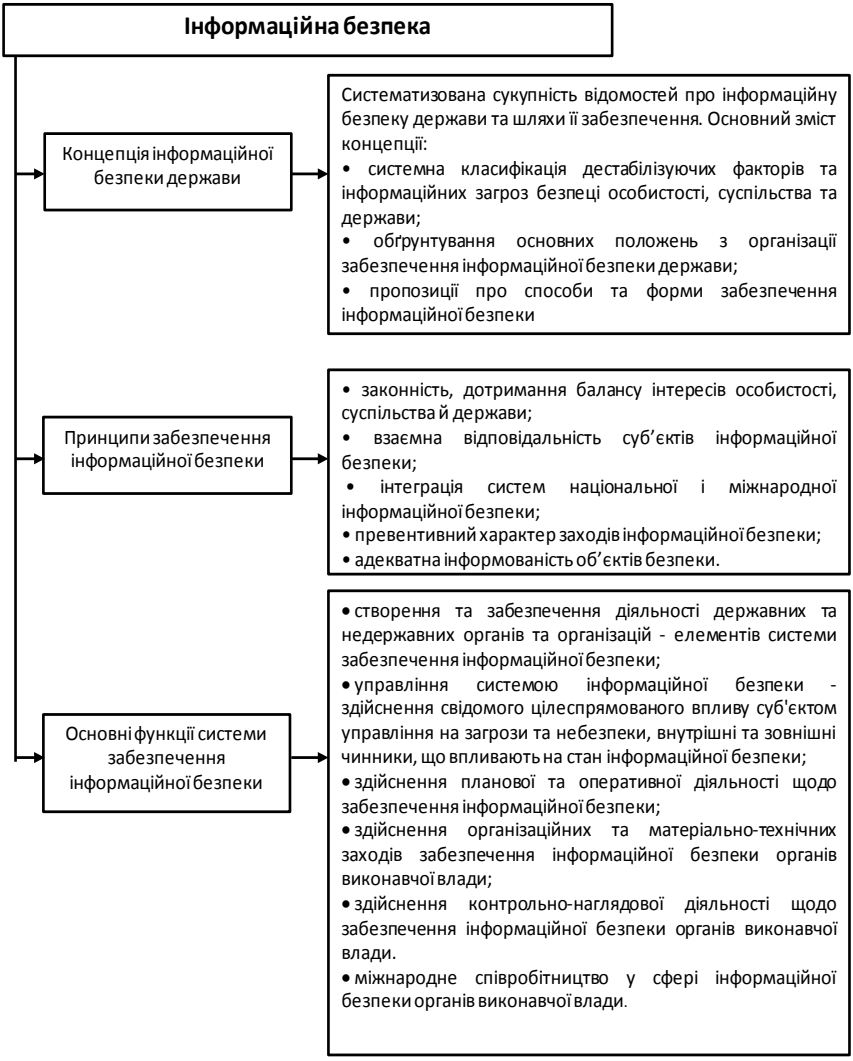


Рис. 6.1. Сутність системи забезпечення інформаційної безпеки

Виходячи з окреслених принципів, формуються і функції СЗІБ, що полягають у наступному:

1. Створення та забезпечення діяльності державних та недержавних органів та організацій – елементів СЗІБ, що включає:

– розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки (доктрини інформаційної безпеки, організаційної та функціональної структури системи);

– системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення всієї системи органів виконавчої влади;

– розробка й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та вдосконалення механізмів реалізації правових норм чинного законодавства.

2. Управління СЗІБ безпеки – здійснення свідомого цілеспрямованого впливу суб'єктом управління на загрози та небезпеки, внутрішні та зовнішні чинники, що впливають на стан інформаційної безпеки:

– розроблення на підставі доктрини інформаційної безпеки конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного рівня органу виконавчої влади, зокрема для центральних та місцевих органів виконавчої влади;

– здійснення прогнозування, планування, організації, регулювання та контролю всією системою інформаційної безпеки та окремими її елементами;

– оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки;

– оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення та застосування ін-

формаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку й ефективного використання інформаційних ресурсів та сприяння доступу уповноважених суб'єктів управління до світових інформаційних ресурсів, глобальних інформаційних систем.

3. Здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки:

– визначення інтересів кожного міністерства, іншого центрального та місцевого органу виконавчої влади в інформаційній сфері та їх пріоритетності відповідно до державної інформаційної політики;

– діагностування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків у разі настання із відпрацюванням відповідних превентивних заходів;

– визначення та здійснення повноважень органів виконавчої влади щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;

– забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів системи органів виконавчої влади.

4. Здійснення організаційних та матеріально-технічних заходів забезпечення інформаційної безпеки органів виконавчої влади:

– розробка й реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів;

– здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесі діяльності органів виконавчої влади;

– введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності органів виконавчої влади (крім інформаційних ресурсів,

що мають відомості, віднесені до державної таємниці та до іншої інформації з обмеженим доступом);

– забезпечення захисту системи органів виконавчої влади від хибної, спотвореної та недостовірної інформації;

– інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами;

– кадрове забезпечення функціонування системи органів виконавчої влади національними інформаційними ресурсами;

– забезпечення розробки та застосування організаційних та економічних механізмів стосовно форм і засобів обігу інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг).

5. Здійснення контрольно-наглядової діяльності щодо забезпечення інформаційної безпеки органів виконавчої влади:

– забезпечення ефективного використання інформаційних ресурсів у діяльності органів виконавчої влади;

– контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів;

– нагляд за додержанням законодавства у сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

6. Міжнародне співробітництво у сфері інформаційної безпеки органів виконавчої влади:

– розробка нормативно-правової бази, що регулює інформаційні відносини між державами та їхню взаємодію в галузі інформаційної безпеки;

– входження до існуючих та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на розв'язання проблем інформаційної безпеки з урахуванням національних інтересів України;

– участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів;

– регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного і взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну, здійснення єдиної державної політики наукової підтримки органів виконавчої влади всіх рівнів, розвитком і використанням національних інформаційних ресурсів.

Неабияку роль у досягненні інформаційної безпеки держави грає інституційний механізм її забезпечення. Ефективність інституціональної системи, що реалізує суспільні інтереси, є запорука їхньої гармонізації в цілях забезпечення вищих державних інтересів, у тому числі національної та інформаційної безпеки.

Інституціональний механізм забезпечення інформаційної безпеки представляє собою окрему структурну складову господарюючого механізму, забезпечуючи створення норм і правил, які регулюють взаємодію різних економічних суб'єктів в інформаційній сфері із запобігання загроз інформаційній безпеці. Інституціональний механізм приводить у дію інститути (формальні та неформальні), розробляє взаємодію суб'єктів, здійснюючи контроль над дотриманням установлених норм і правил.

Таким чином, інституційний механізм забезпечення інформаційної безпеки включає в себе відкриту основу та забезпечує її інституційні структури. Удосконалення даного механізму включає в себе реорганізаційну основу інформаційної безпеки та інституціональних сигналів протидіям загроз інформаційної безпеки.

В інституціональний механізм забезпечення інформаційної безпеки входить:

– прийняття нових законів, що висвітлювали б інтереси всіх суб'єктів інформаційної сфери;

– дотримання балансу виробничої й обмежувальної функції законів в інформаційній сфері;

– інтеграція України у світовий правовий простір;

– облік стану сфери сучасних інформаційних технологій.

Система правового регулювання інформаційної безпеки, у свою чергу, включає масив правових норм, що регулюють відносини в даній сфері, правовідносини, що виникають на основі застосування правових норм, та відповідні правозастосовчі акти. Правові норми складають базу забезпечення інформаційної безпеки і визначають ефективність діяльності держави, суспільства та окремих громадян із захисту національних інтересів України в інформаційній сфері. До складу цієї бази включаються й норми міжнародних договорів України, закони України, акти Президента України, постанови уряду, нормативні акти органів державної влади, які регулюють відносини в даній сфері. Аналіз стану нормативно-правового регулювання забезпечення інформаційної безпеки України показує, що інформаційну безпеку України становлять три структурні елементи (рис. 6.2.):

1. Інформаційна безпека у сфері прав і свобод людини та громадянина – управління реальними чи потенційними загрозами з метою забезпечення права на інформацію. Зміцненню в Україні цілісного механізму захисту прав і свобод людини, такого, що відповідає новітнім викликам і загрозам інформаційній безпеці, перешкоджають чинники, які склалися на практиці, зокрема: корпоративний опір носіїв влади незалежній правозахисній діяльності, проблеми свободи ЗМІ, відсутність належного рівня правової інформованості в суспільстві й неконструктивне суперництво між суб'єктами правозахисної діяльності, що мають єдину або різну правову природу. Подолання деструкції такої конкуренції – завдання, що найбільш складно вирішується, оскільки цього не можна досягти за простим велінням [4].

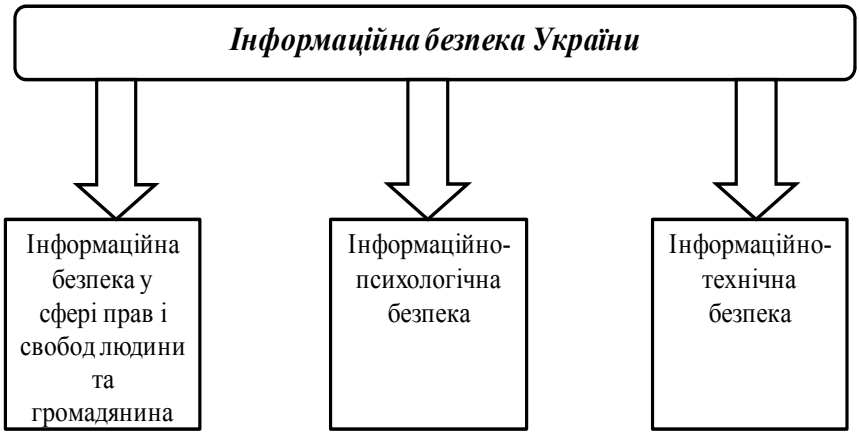


Рис. 6.2. Елементи забезпечення інформаційної безпеки України

2. Інформаційно-психологічна безпека – управління реальними чи потенційними загрозами, що можуть завдати шкоди психіці людини, суспільства. В умовах сьогодення все більше дослідників звертають увагу на необхідність активної розробки проблематики інформаційної і психологічної безпеки особистості, суспільства й держави. Сам процес суспільного розвитку висуває ці проблеми в число першочергових. Це обумовлено тим, що без їхнього вирішення неможливий подальший сталий суспільний розвиток і забезпечення безпеки особистості, суспільства й держави в політичній, економічній, соціальній, духовній, військовій та інших областях.

3. Інформаційно-технічна безпека – управління потенційними чи реальними загрозами з метою захисту комп'ютерних, телекомунікаційних технологій та інших технологій зв'язку. Проблеми інформаційно-технічної безпеки починають посідати одне з ключових місць у системі забезпечення реалізації всіх політико-правових проблем, стають життєво важливими при реалізації інтересів усіх без винятку осіб, суспільств і країн.

Вони стають ключовою організаційно-управлінською та регулятивно-контрольною функцією в діях усіх владних структур, оскільки порушення нормального функціонування інформаційних та телекомунікаційних систем становлять собою серйозну небезпеку, що обумовлює нагальну потребу створення нових, більш досконалих адміністративно-правових норм інформаційно-комунікаційної діяльності в державі.

Нормативно-правові засади побудови, поточної діяльності та розвитку СЗІБ України на сьогодні складають такі документи: Конституція України, Закон України «Про інформацію», Закон України «Про основи національної безпеки України», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про державну таємницю», Закон України «Про Національну програму інформатизації», Закон України «Про захист персональних даних», Указ Президента України «Про Доктрину інформаційної безпеки України», Концепція національної безпеки України та інші законодавчі та нормативно-правові акти, що регулюють суспільні відносини в інформаційній сфері.

Нормативно-правове підґрунтя має досить розвинений характер, оскільки більшість норм відповідають міжнародним стандартам, принципам і нормам забезпечення прав і свобод людини та громадянина, зокрема права на свободу слова, отримання та поширення інформації. Водночас системні проблеми даються взнаки і при вирішенні галузевих проблем, тому несформованість нормативно-правової бази щодо регулювання суспільних відносин у сфері національної безпеки, відповідним чином негативно впливає на можливість формування достатньої й ефективно діючої нормативно-правової бази з питань забезпечення національної безпеки в інформаційній сфері.

Серед завдань правового забезпечення особливу увагу слід звернути на ті, які найбільшою мірою розкривають його зміст. До них слід віднести:

– визначення ризиків інформаційної безпеки особистості, суспільства й держави;

– закріплення на законодавчому рівні національних інтересів;

– визначення основних напрямків забезпечення національної та інформаційної безпеки в різних сферах життя суспільства;

– створення організаційних основ системи забезпечення національної та інформаційної безпеки (визначення основних завдань, принципів організації, внутрішньої структури, сил і засобів, місця в механізмі держави, закріплення функцій і розмежування повноважень органів держави, що входять до системи забезпечення національної та інформаційної безпеки);

– забезпечення балансу інтересів особистості, суспільства й держави у сфері забезпечення національної та інформаційної безпеки;

– встановлення та реалізація юридичної відповідальності за протиправні дії, що посягають на безпеку особистості, суспільства й держави;

– формування системи попередження правопорушень у сфері національної та інформаційної безпеки;

– правове виховання і формування правосвідомості громадян і посадових осіб, зорієнтовані на забезпечення національної та інформаційної безпеки.

Основними елементами організаційної основи СЗІБ України є такі суб'єкти: Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки й оборони України, органи виконавчої влади України, міжвідомчі й державні комісії, створені Президентом України та Кабінетом Міністрів України, органи місцевого самоврядування, органи судової влади, громадські об'єднання, громадяни, що беруть участь відповідно до законодавства України у вирішенні завдань забезпечення інформаційної безпеки України. Наглядний взаємозв'язок цих елементів схематично представлено на рис. 6.3. [25].

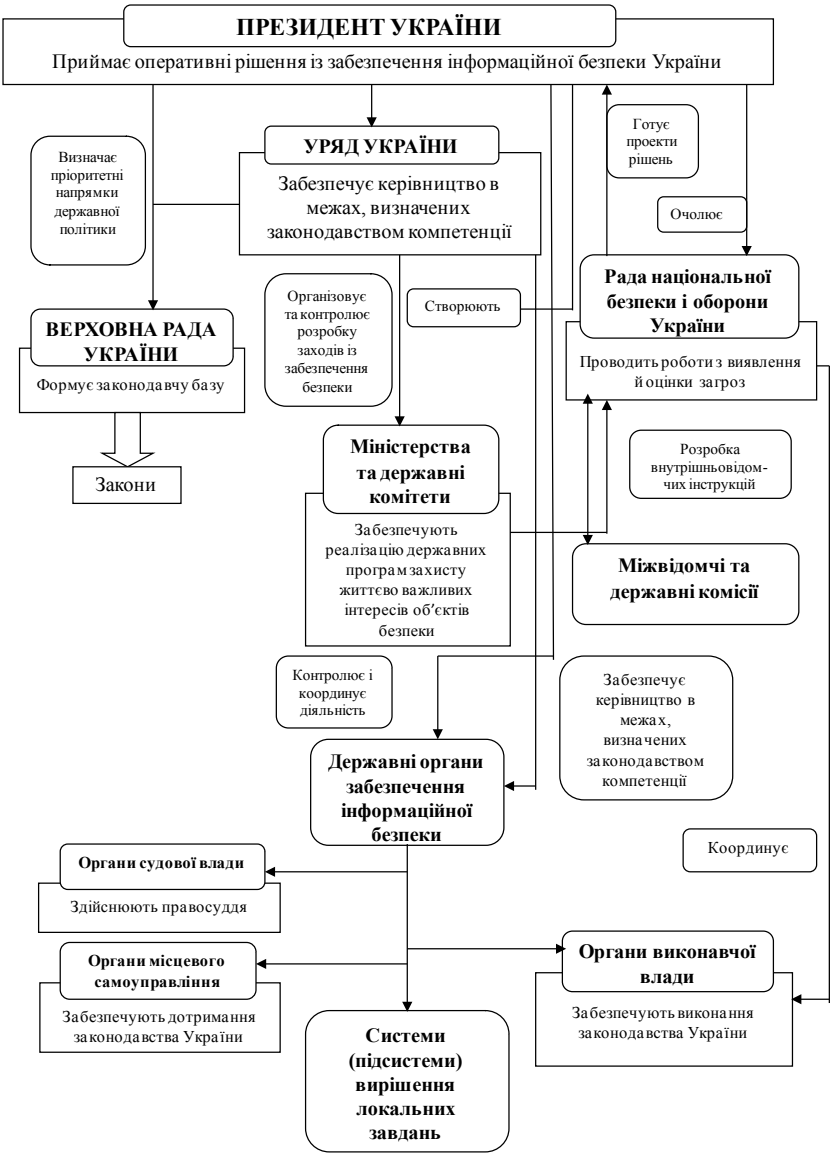


Рис.6.3. Елементи організаційної основи системи забезпечення інформаційної безпеки України

Суб'єкти СЗІБ України мають тісно взаємодіяти між собою, водночас кожний із них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції, уживаючи при цьому відповідних, визначених законом, адміністративно-правових форм та методів. У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, унаслідок чого створюють стрункy організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією із забезпечення інформаційної безпеки.

Об'єктами системи забезпечення інформаційної безпеки України є:

– інтереси органів державного управління в інформаційній сфері;

– система органів державного управління, а також їхні компетентні особи і відносини між ними (суспільні відносини в інформаційній сфері);

– власне система забезпечення інформаційної безпеки України [3].

Із певною долею умовності можна говорити про те, що в Україні в основному створено законодавчу основу забезпечення інформаційної безпеки, що включає сукупність основних нормативних правових актів, які містять юридичні принципи й норми, спрямовані на правове врегулювання суспільних відносин у сфері забезпечення інформаційної безпеки держави. Разом із тим правова база регулювання відносин у цій сфері ще далека від досконалості, що пов'язано з формуванням нової структури економічних, політичних, соціальних і духовних реалій як усередині країни, так і на міжнародній арені. У законодавстві не відображені реальні й дієві правові механізми адекватної протидії новим ризикам інформаційної безпеки. Потребують уточнення й класифікації сфери діяльності держави щодо її забезпечення. Протиріччя, подвійне тлумачення та декларативність положень відповідних законів перешкоджають їхньому ефективному й цілеспрямованому виконанню.

Із огляду на викладене, випливає, що першочерговим завданням для законодавця є формування гнучкої правової системи інформаційної безпеки держави, яка б комплексно врегулювала дану сферу відносин і відобразила державну політику у сфері забезпечення інформаційної безпеки, заходи захисту інформації, види та джерела загроз у сфері інформаційної безпеки, першочергові заходи щодо забезпечення інформаційної безпеки.

6.2. Сучасні нормативно-правові документи у сфері забезпечення інформаційної безпеки

Проблема забезпечення інформаційної безпеки є на сьогодні однією з найгостріших не лише в нашій країні, але й у розвинених країнах світу.

Нинішній стан інформаційної безпеки України – це стан нового, що тільки формується з урахуванням веління часу. Багато чого вже зроблено, але ще є проблеми, що вимагають найоперативнішого вирішення.

Як уже зазначалось вище, інформаційна безпека є складовою національної безпеки України, що забезпечує захист системи публічного управління від інформаційно-комунікаційних загроз та викликів, у той же час сама система публічного управління забезпечує суспільство, державу та громадян інформаційно-якісними послугами та якісною інформацією. Тобто система інформаційної безпеки носить двосторонній характер: зовнішній та внутрішній – і захищає себе та інших від неякісної інформації, інформаційних атак тощо.

Найважливіше завдання в справі забезпечення інформаційної безпеки держави – здійснення комплексного врахування національних інтересів особистості, суспільства й держави в даній сфері (рис. 6.4.).

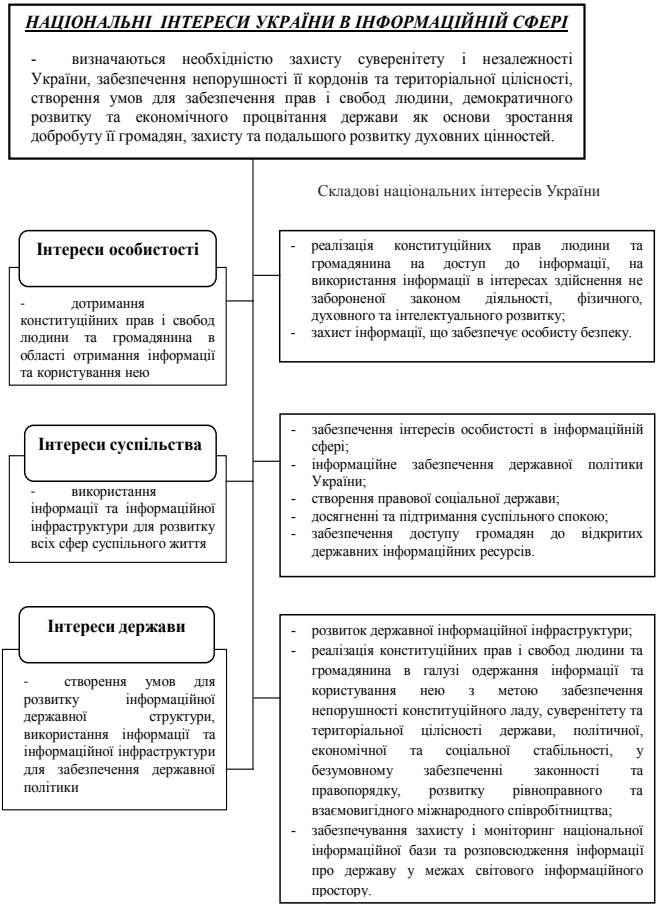


Рис. 6.4. Національні інтереси України в інформаційній сфері

Дотримання принципу балансу інтересів громадян, суспільства й держави в інформаційній сфері передбачає законодавче закріплення пріоритету цих інтересів у різних областях життєдіяльності суспільства, а також використання різних форм громадського контролю над діяльністю органів державної влади. Реалізація гарантій конституційних прав і свобод людини й громадянина, що стосуються діяльності в інформаційній сфері,

є найважливішим завданням держави в галузі інформаційної безпеки [5].

Чинне законодавство України не містить відповідного розгорнутого тлумачення поняття «інформаційна безпека держави», проте нормативні акти, які торкаються питань інформаційної безпеки, закономірно розглядають її в контексті більш загального поняття національної безпеки. Такий підхід значно обмежує та звужує зміст категорії «інформаційна безпека держави», позаяк виключно інформаційний простір слугує каналом реалізації загроз національній безпеці в усіх сферах діяльності держави. Термін інформаційної безпеки закріплено лише у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [6].

Як зазначено у Законі України «Про національну безпеку», державна політика у сферах національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо [7].

Однак національний інформаційний простір України, на превеликий жаль, зазнає суттєвих загроз, викликів, що становлять небезпеку функціонування держав, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури [8].

У Доктрині інформаційної безпеки України визначено, що до національних інтересів України в інформаційній сфері віднесено такі життєво-важливі інтереси особи, як забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів.

Також у ній зазначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ та ме-

режу Інтернет; деструктивні інформаційні впливи, що спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ та в мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [9].

Однак цей документ являє собою сукупність теоретичних понять про цілі, принципи та правові складові інформаційної безпеки. Відтак, із нього не зрозуміло чітких завдань та відповідальних суб'єктів за інформаційну безпеку, оскільки він є лише основою для розроблення проєктів, концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України.

Інформаційна безпека України – передбачений Конституцією захист політичних, державних, громадських інтересів країни, загальнолюдських і національних цінностей [10]. Важливість забезпечення інформаційної безпеки задекларована в ст.17 Конституції України [11] як одна із найважливіших функцій держави та справа всього Українського народу поряд із захистом суверенітету, територіальної цілісності України та економічною безпекою.

У сучасних умовах найважливішим елементом інформаційної безпеки є кібербезпека. Про пріоритетність забезпечення кібербезпеки в України свідчить запроваджена в 2016 році Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 [12]. Отже, початок регулюванню інформаційної безпеки в Україні покладено, що однозначно є позитивним кроком. Однак шляхи реалізації прийнятих норм на практиці розробляються дуже повільно та в більшості випадків не служать правовим інструментом для практичного застосування та забезпечення ефективності заходів кібербезпеки.

Основною метою державного управління є розробка та реалізація концептуальних основ державної інформаційної політики шляхом прийняття адекватних нормативно-правових

актів щодо врегулювання інформаційних відносин [1]. Останнім часом значно зросла необхідність у комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору, що наглядно представляється в нормативних документах закордонних країн. У провідних країнах світу протягом десятиліть створювалося законодавство з інформаційної політики та інформаційної безпеки і, як засвідчує їхній досвід, великого значення для нормального функціонування інформаційної сфери держави набуває узгоджена діяльність відповідного державно-правового механізму, тобто система взаємопов'язаних державних органів, організацій, установ щодо вироблення та реалізації сукупності норм та принципів права, які повинні врегулювати суспільні відносини в інформаційній сфері [13].

Наприклад, у Молдові діє Стратегія інформаційної безпеки, що містить опис безпечних та правових проблем, цілі, задачі, ключові показники ефективності (KPI), план реалізації з чітким розподілом відповідальних суб'єктів. У Данії теж на державному рівні розроблено стратегію інформаційної та кібербезпеки, що комплексно охоплює питання реалізації – від найвищого державного рівня до безпеки людини в мережі. В Естонії, яка вважається європейським лідером із застосування цифрових технологій в економіці та адмініструванні, дбають про інформаційний захист із 1996 року.

Для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства й забезпечення інформаційної безпеки [14]. Зважаючи на вищесказане, можна запропонувати необхідні перші кроки для посилення інформаційної безпеки (рис. 6.5.):

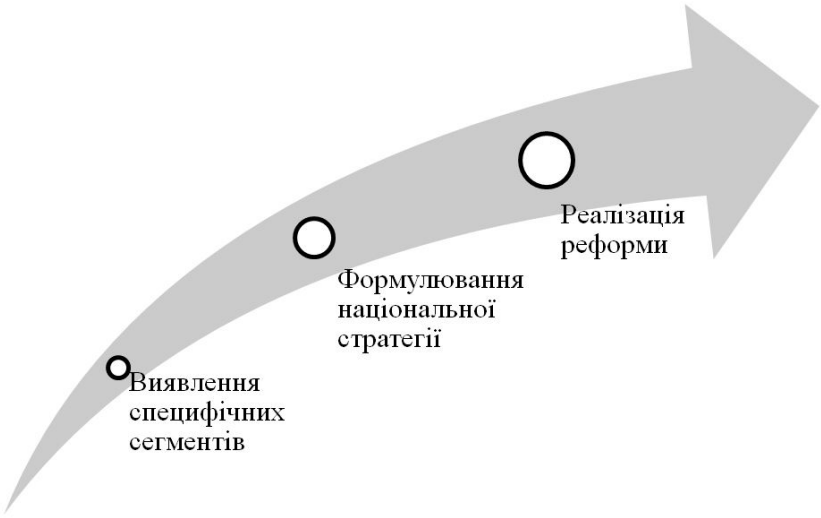


Рис. 6.5. Ключові кроки модернізації інформаційної безпеки

1. Виявити специфічні сегменти, що вимагають реформування у сфері інформаційної безпеки, для цього провести комплексні аудити (правовий, технічний, комунікаційний та освітній) у сфері інформаційної безпеки в державних органах із залученням зацікавлених суб'єктів.

2. Сформувати національну стратегію інформаційної безпеки та реалістичний план її виконання на основі виявлених уразливостей разом із фахівцями у сфері інформаційної безпеки.

3. Розпочати реалізацію реформи інформаційної безпеки з урахуванням змін обстановки, характеру та змісту загроз національній безпеці України в інформаційній сфері, умов реалізації державної інформаційної політики та формування національного інформаційного простору [6].

Виходячи з вище зазначеного, можна стверджувати, що рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз – це завдання шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо. На жаль, нині в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Разом із тим процес інформатизації має стихійну, некеровану природу з переважним ухилом у бік використання засобів інформатизації іноземного виробництва, а тому окреслені кроки модернізації інформаційної безпеки є вкрай необхідними для розбудови міцної національної безпеки та конкурентоспроможності країни щодо ефективного використання ресурсів (із урахуванням їх якості).

6.3. Правовий захист громадян у сфері інформаційної безпеки

У першому розділі монографії було розглянуто потреби особистості на інформаційну безпеку та представлено суспільний запит на останню, що підкреслює актуальність розбудови даної галузі держави. Власне, теоретичне осмислення дії правового механізму захисту інформаційних прав і свобод украй важливе питання, бо тут не можна обійтися лише аналізом і коментуванням чинного законодавства в цій сфері. Необхідно системне теоретико-правове обґрунтування та дослідження цієї злободенної правової проблеми.

Права людини є фундаментом сучасної правової держави. На постіндустріальному етапі розвитку захист прав людини набуває особливого характеру. Удосконалення інформаційно-комунікаційних технологій супроводжується розширенням можливостей їхнього недобросовісного використання, яке створює загрози інформаційній безпеці та може призвести до порушень

прав людини. У зв'язку з цим виникає проблема співвідношення інформаційної безпеки і прав людини, передусім, права на недоторканість приватного життя [15].

Співвідношення свободи і відповідальності, прав і обов'язків у взаємовідносинах громадянина та держави неможливе без інформаційного забезпечення. Інформація стає фактором успішного та стабільного розвитку як суспільства в цілому, так і його членів – суб'єктів суспільних відносин, які отримують, використовують і поширюють інформацію. Інформаційні права, таким чином, мають як власне юридичну, так і загальносоціальну значимість. Інформація, інформаційні права надають можливість забезпечувати взаємно необхідні відносини громадянина й держави.

Інформаційні права і свободи вбудовані в загальну систему прав і свобод. Це означає, що осмислення й дослідження питань дії правового механізму захисту інформаційних прав і свобод позитивно впливає на вивчення й організацію правової охорони та захисту прав і свобод людини й громадянина в Україні в цілому.

Правова форма захисту інформації – це захист інформації, який «базується на використанні статей Конституції і законів держави, положень цивільного і кримінального кодексів та інших нормативно-правових документів у галузі інформатики, інформаційних відносин та інформації. Вона регламентує права й обов'язки суб'єктів інформаційних відносин, правовий статус органів, технічних засобів і способів захисту інформації і є базою для створення морально-етичних норм в області захисту інформації» [16].

В Україні захистом прав і свобод людини й громадянина зайняті багато структур, де особливе місце посідають Президент України, законодавчі та виконавчі органи, правозастосовні структури. Правозахисні об'єднання, ініціативи депутатів, а також громадян, зацікавлених в об'єктивному й справедливому вирішенні того чи іншого питання, також мають свій помітний,

деколи вирішальний вплив у вирішенні питань захисту прав і свобод людини й громадянина в Україні [17, 18].

Діяльність усіх органів і структур, що забезпечують або впливають на характер захисту прав і свобод людини й громадянина, безумовно, потребує стабільного й надійного функціонування правового механізму захисту прав і свобод людини й громадянина в державі.

Як уже зазначалося, в Україні поняття «безпека», «інформаційна безпека» і «національна безпека» розкриваються через стан захищеності життєво важливих інтересів особи, суспільства й держави. Слід підкреслити, що захист від неправомірного інформаційного втручання є дуже важливим аспектом інформаційної безпеки особи, оскільки, на відміну від порушень свободи слова, подібне втручання може мати прихований характер, але, разом із тим, створювати значну загрозу.

На думку А. Нашинець-Наумової, важливим підґрунтям удосконалення інформаційного законодавства є адекватне сучасним умовам відображення у свідомості нормотворців інформаційної безпеки у всій повноті аспектів, зокрема психологічному, технічному та правовому [19].

Одним із основних пріоритетів інформаційної політики будь-якої країни є дотримання балансу відповідних інтересів особистості, суспільства й держави. Але країни, що обрали демократичний шлях розвитку, принципово виходять при цьому з примату прав і свобод особистості. На нормативному рівні це зазвичай виражається в конституційних гарантіях свободи слова та доступності інформації для кожного громадянина. Реалізація цих прав у практичному вимірі передбачає дотримання двох базових принципів:

1. Свобода публічних висловлювань незалежно від їхнього політичного змісту;

2. Забезпечення безперешкодного отримання громадянами повної та неупередженої інформації. Обмеження цього фундаментального права особистості розглядається як виняток

із загального принципу відкритості інформації та реалізується тільки відповідно до чинного законодавства і лише в окремих випадках [19, 20].

Загалом вітчизняна законодавча база у своїх основах відповідає духу та букві основних міжнародно-правових актів у сфері інформації й продовжує вдосконалюватись. Так, 17 грудня 2008 р. Верховна Рада України ратифікувала Європейську конвенцію про транскордонне телебачення [21], а в 2017 році Указом Президента України було затверджено Доктрину інформаційної безпеки України [9]. У Доктрині визначено національні інтереси України в інформаційній сфері, у ній інформаційна безпека розглядається як стан захищеності національних інтересів України в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства й держави, від внутрішніх і зовнішніх загроз.

Конституція України містить цілий комплекс прав і свобод людини й громадянина, що визначають її правовий статус у сфері інформаційних відносин. Як зазначено в статті 3, «людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їхні гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження та забезпечення прав і свобод людини є головним обов'язком держави» [11]. Також ключовими в цьому аспекті, безумовно, є норми статті 34 Конституції. Так, стаття 34 визначає: «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань» [11]. Крім загального визначення права людини на інформацію, у ст.34 Конституції є ряд інших інформаційних прав і свобод, що закріплюються конституційними нормами:

1. Свобода особистого та сімейного життя (ст. 32: «…не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випад-

ків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»).

2. Таємниця листування, телефонних переговорів, телеграфної й іншої кореспонденції (ст. 31: «…винятки можуть бути встановлені лише судом у випадках, передбачених законом, із метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо»).

3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе (ст. 32: це стосується відомостей, що «не є державною або іншою захищеною законом таємницею»).

4. Право громадянина направляти індивідуальні або колективні письмові звернення чи особисто звертатися до органів державної влади, органів місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40).

5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про її стан (ст. 50: «…така інформація ніким не може бути засекречена»).

6. Право кожного на свободу творчості та право доступу до культурних цінностей (ст. 54: результати інтелектуальної, творчої діяльності громадянина «ніхто не може використовувати або поширювати їх без його згоди, за винятками, установленими законом»).

7. Право кожного громадянина на одержання кваліфікованої правової допомоги (ст. 59: «…у випадках, передбачених законом, ця допомога надається безоплатно»).

Утрата зв'язку з вищою цінністю – правами людини для діяльності держави та її органів із забезпечення інформаційної безпеки, будь то правотворча, правоохоронна діяльність, яка створює ризики для порушення відповідних прав. Тому будь-яка

діяльність держави, у тому числі спрямована на забезпечення інформаційної безпеки, повинна ґрунтуватися у своїй вихідній точці на визнанні, дотриманні й захисті прав людини.

Розглядаючи проблеми прав людини при забезпеченні інформаційної безпеки, можна виділити дві складові, які обумовлені різними проявами цієї діяльності й у сукупності дозволяють гарантувати реалізацію прав людини. Перша складова пов'язана з тим, що заходи щодо забезпечення інформаційної безпеки можуть бути безпосередньо спрямовані на захист прав людини. Друга складова заснована на тому, що такі заходи не повинні призводити до обмеження прав людини та повинні бути відповідні загрозам і наслідкам їхнього прояву.

Загрозами інтересам суспільства в інформаційній сфері можуть бути:

– невиконання вимог законодавства, що регулює відносини в інформаційній сфері;

– створення монополій на формування, отримання й поширення інформації в Україні, у тому числі з використанням телекомунікаційних систем;

– дезорганізація та порушення системи накопичення і збереження культурних цінностей, включаючи архіви;

– посилення залежності духовної, економічної та політичної сфер суспільного життя України від зарубіжних інформаційних структур, девальвація духовних цінностей, пропаганда зразків масової культури, заснованих на культі насилля, на духовних і моральних цінностях, що суперечать цінностям, прийнятим в українському суспільстві;

– збільшення відтоку за кордон спеціалістів і правовласників інтелектуальної власності;

– порушення правил у сфері обігу інформації, а саме протиправний збір і використання інформації, порушення технології обробки інформації, витік інформації технічними каналами, знищення, порушення чи крадіжка інформації в мережах передачі даних і на лініях зв'язку, нав'язування оманливої інформа-

ції, несанкціонований доступ до інформації, що знаходиться в банках і базах даних, порушення законних обмежень на поширення інформації;

– порушення правил у сфері функціонування інформаційних систем і у сфері використання засобів забезпечення інформаційної безпеки, а саме: компрометація ключів і засобів криптографічного захисту, використання несертифікованих вітчизняних і зарубіжних інформаційних технологій, засобів захисту інформації, телекомунікацій і зв'язку при створенні й розвитку української інформаційної інфраструктури [22].

Заходи щодо забезпечення інформаційної безпеки, які безпосередньо спрямовані на захист прав людини, можуть носити організаційно-правовий характер, у тому числі вони можуть бути виражені в розвитку державного регулювання та створення необхідної нормативно-правової бази для захисту даних прав. Також вони можуть полягати в реалізації технічних заходів. Однак захист прав людини в обох випадках є основною їхньою метою.

Слід відрізняти загрози інформаційній безпеці від загроз життю, здоров'ю, власності, іншим подібним цінностям у результаті скоєння правопорушень. Загрози інформаційній безпеці можуть мати самостійне значення, наприклад, у випадках, коли їхнім об'єктом є недоторканність приватного життя і втручання, яка призведе до порушення відповідних прав. Також мова може йде про неправомірні дії тих чи інших осіб, при яких порушення інформаційної безпеки не є самоціллю, а лише служить засобом порушення інших видів безпеки. Так, дезінформація в мережі щодо політико-правових подій може бути спрямована на організацію громадських заворушень. Утручання до функціонування інформаційних систем може бути причиною збою окремих систем забезпечення життєдіяльності.

Коли порушення інформаційної безпеки не є самоціллю, загрози власне інформаційної безпеки стають передумовою загрозам, що відповідають «не – інформаційним» цінностям. У

зворотному випадку можна говорити про загрози безпеці життя, здоров'я, економічної безпеки, але не про загрози інформаційній безпеці. При порушенні інформаційної безпеки неправомірний акт, пов'язаний із реалізацією загроз інформаційним цінностям, повинен передувати порушенню права на життя, здоров'я, власність і т.ін. Друга складова проблеми прав людини при забезпеченні інформаційної безпеки пов'язана з відповідністю застосованих заходів щодо виявлення, попередження та усунення загроз безпеки, локалізації та нейтралізації наслідків їхнього прояву.

Технічні й технологічні вразливості, як правило, виявляються та усуваються з використанням таких же по суті технічних рішень. Уразливість з боку людини, що бере участь у системі забезпечення інформаційної безпеки, включає, з одного боку, прийняття організаційно-правових заходів, які пов'язані з покладанням на дану людину деяких обов'язків і відповідними можливостями вимагати від неї активної поведінки, а з іншого боку– здійснення контролю за діями даної людини. Але оскільки контроль у більшості випадків здійснюється також людиною, то сфера контролю стає тотальною.

Тотальний контроль при забезпеченні інформаційної безпеки, по суті, заснований на припущенні, що кожна дія й кожна подія потенційно створює загрозу її порушення. Подібне припущення дозволяє застосовувати до фізичних осіб заходи контролю, засновані на свого роду «презумпції потенційної винуватості», і, таким чином вторгатися у сферу приватного життя. Керування даним припущенням призводить до того, що обмеження прав людини на недоторканність приватного життя, особисту таємницю, таємницю листування і т.ін. починають проникати все глибше в правове регулювання і ставати повсюдними. Саме тому розвиток більшої частини існуючих систем забезпечення інформаційної безпеки поступово перетворюється на систему тотального стеження за всіма учасниками системи, при цьому з поступовим виходом за межі даної системи.

Проблема тотального контролю при забезпеченні інформаційної безпеки з'явилася відносного недавно, у кінці XX століття, і викликана не тільки розвитком технічних можливостей, але також випадками актів тероризму, що призводять до масових жертв. Протидія даним загрозам вимагає посилення державної влади. При цьому можна сформулювати наступне правило: чим більший дисбаланс влади, тим більше потрібен захист приватного життя.

Вплив сучасних інформаційно-комунікаційних технологій проявляється, насамперед, у сфері особистих прав, серед яких особливе місце займає право на недоторканність приватного життя. Слід погодитися з твердженням, що «без інформаційної безпеки не може бути недоторканності приватного життя». Порушення прав людини, що виразилося в незаконному зборі, зберіганні, обробці, наданні та поширенні інформації про нього, може стати засобом для більш тяжких правопорушень незалежно від того, відбуваються вони від приватних осіб або державних органів. Держава завжди більш оперативно реагує на можливості, яких надають нові інформаційно-комунікаційні технології для захисту публічних, ніж приватних інтересів. При цьому вони об'єктивно прагнуть до посилення даних можливостей і схильні тлумачити їх розширено, що, у свою чергу, може призводити до обмеження прав людини.

Важливим елементом механізму забезпечення права людини на конфіденційність приватного життя може розглядатися встановлене ст. 31 Закону «Про інформацію» право громадян на доступ до інформації про них, зібраної органами державної влади та місцевого самоврядування. Це право (ч.1. ст.31) включає в себе право громадян знати в період збирання інформації, які відомості про них і з якою метою збираються, як, ким і з якою метою вони використовуються; та право громадян мати доступ до інформації про них, і, у разі необхідності, заперечувати її правильність, повноту, доречність тощо [23].

Основними принципами для встановлення обмежень прав людини, закріпленими в більшості конституцій і ряді міжнародних угод, які гарантують реалізацію прав людини, є «встановлення обмеження тільки законом» і «необхідність у демократичному суспільстві». При цьому такий принцип як «необхідність у демократичному суспільстві» є оціночним і застосовується вже після встановлення обмеження.

Вторгнення в приватне життя з метою забезпечення інформаційної безпеки може бути виражене в зборі, обробці, зберіганні, наданні або поширенні інформації про приватне життя особи, забезпеченні доступу до неї. Навіть за наявності закону, яким установлено відповідне обмеження, і обґрунтованості мети його введення «необхідністю» в демократичному суспільстві, перевірці також підлягає відповідність способів реалізації обмеження цілям його встановлення. Оцінка відповідності з цим принципом дозволяє не тільки визначити доцільність або обґрунтованість такого обмеження, але також оцінити можливість ефективного досягнення тих же цілей у відсутності обмеження права або його меншому обмеженню. Наскільки подібне вторгнення є обґрунтованим і «необхідним у демократичному суспільстві», залежить від численних факторів, які поки слабо піддаються формалізації і можуть казуїстично трактуватись у практиці національних судів, перш за все, конституційної юстиції і рішеннях Європейського суду з прав людини.

У даних умовах гарантією реалізації права людини на недоторканність приватного життя повинна служити система вживаних державою заходів, не тільки спрямованих на захист прав людини безпосередньо шляхом забезпечення інформаційної безпеки, але також і таких, що дозволяють своєчасно виявляти факти невідповідності обмежень прав людини загрозам інформаційної безпеки та наслідків їх прояву. Як відзначають у зарубіжній літературі, «забезпечення недоторканності приватного життя не повинно обмежуватися тим, що законодавці, судді та державні службовці надають їй достатньої уваги. Вони також

повинні забезпечити постійний контроль для того, щоб переконатися, що недоторканність приватного життя може відігравати важливу роль у якості противаги перед обличчям нових загрозливих подій».

Сучасні технології створюють можливості не тільки для їхнього недобросовісного використання, але також і для попередження, виявлення та припинення адміністративних правопорушень і злочинів. Однак порушення права людини на недоторканність приватного життя може статися в обох випадках незалежно від мети використання відповідних технологій. У зв'язку з цим необхідні не тільки подальше вироблення і вдосконалення заходів забезпечення інформаційної безпеки, спрямованих на захист прав людини, а й створення системи контролю та нагляду, яка б дозволяла своєчасно виявляти факти невідповідності обмежень прав людини загрозам інформаційної безпеки та наслідків їхнього прояву.

Загальним висновком може слугувати нагадування про те, що сфера інформаційної безпеки людини та суспільства є дуже тонкою і відповідальною. З одного боку, вона вимагає втручання держави з метою забезпечення необхідного рівня безпеки й уникнення суспільно небезпечного та непередбачуваного розвитку інформаційних відносин. З іншого боку, надмірне державне втручання саме по собі створює загрозу та може призвести до негативних наслідків, обмеження прав людини й руйнації демократичних інститутів громадянського суспільства.

Список використаних джерел

1. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ. 2006. 280 с.

2. Стрельцов А.А. Направление совершенствования правового обеспечения информационной безопасности Россий-

ской Федерации. Информационное общество. 1999. № 6. С. 15-21.

3. Ліпкан В.А. Національна безпека України: навчальний посібник. Київ: КНТ. 2009. 576 с. URL : http://politics.ellib.org.ua/pages-8286.html (дата звернення: 10.03.2020).

4. Настюк В.Я, Бєлєвцева В.В Правовий захист інформаційних прав і свобод людини в Україні: проблеми та перспективи. Інформація і право. № 2(14). 2015. URL: http://ippi.org.ua/sites/default/files/nvybvvpzips_14_2_2015.pdf (дата звернення: 10.03.2020).

5. Панченко О.А. Законотворча діяльність у сфері національної безпеки. Державне управління: удосконалення та розвиток. Київ. № 3. 2020. DOI: 10.32702/2307-2156-2020.3.7. URL:http://www.dy.nayka.com.ua/?op=1&z=1594 (дата звернення: 20.03.2020).

6. Апетик А. Інформаційна безпека. 2019. URL:https://webcache.googleusercontent.com/search?q=cache:nY_TI2_Dяn-8J URL: https://www.prostir.ua/%3Flibrary%3Dinformatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje+&cd=3&hl=ru&ct=clnk&gl=ua. (дата звернення: 10.03.2020).

7. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text. (дата звернення: 10.03.2020).

8. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки. Вип. 2. № 1. 2016. С. 27–32.

9. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47. 2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text. (дата звернення: 20.03.2020).

10. Панченко О.А. Проблеми правового забезпечення державного управління інформаційною безпекою. Державне

управління: удосконалення та розвиток. Київ. № 11. 2019. DOI: 10.32702/2307-2156-2019.11.3. URL: http://www.dy.nayka.com.ua/?op=1&z=1561 (дата звернення: 21.04.2020).

11. Конституція України. Верховна Рада України; Закон України; Закон від 28.06.1996 №254к/96-ВР. URL:https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. (дата звернення: 10.03.2020).

12. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року. «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16#Text. (дата звернення: 10.03.2020).

14. Малик Я.Й., Береза О.І. Забезпечення інформаційної безпеки України у контексті світового досвіду. Ефективність державного управління. 2012. Вип. 32. С. 20–27.

15. Богуш В.М., Юдін О.К. Інформаційна безпека держави. К. : МК-Прес. 2005. 432 с.

16. Панченко О.А. Суспільно значущі фактори державної інформаційної безпеки. Публічне управління і адміністрування в Україні. 2020. Випуск 16. С.116-120. URL: http://www.pag-journal.iei.od.ua/archives/2020/16-2020/22.pdf (дата звернення: 21.04.2020).

17. Домарев В.В. Безопасность информатизационных технологий. Методология создания системы защиты. К. : ООО «ТИД «ДС» 2001. С. 650.

18. Фурашев В.М. Законодавче забезпечення інформаційної безпеки україни. Інформація і право. 2014. № 1(10). URL : http://ippi.org.ua/sites/default/files/14fvmibu.pdf (дата звернення: 20.03.2020).

19. Присяжнюк М., Бєлошевич Я. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету ім. Т. Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 29–33.

20. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Київ: «Гельветика». 2017. URL: http://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf (дата звернення: 21.04.2020).

21. «Дотримання інформаційних прав і свобод українських громадян: нормативно-правове забезпечення і регулятивні важелі». Аналітична записка. URL: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/dotrimannya-informaciynikh-prav-i-svobod-ukrainskikh-gromadyan (дата звернення: 20.03.2020).

22. Європейська конвенція про транскордонне телебачення (укр/рос) (ETS № 132) Рада Європи; Конвенція, Міжнародний документ від 05.05.1989 № ETS (132). URL: https://zakon.rada.gov.ua/laws/show/994_444#Text. (дата звернення: 21.04.2020).

23. Кохановська О.В. Інформаційно–правова основа громадянського суспільства. Право України. 2015. № 4. С.35-42.

24. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис… д-ра юрид. наук ; 12.00.07. Харків: НУВС. 2004.

25. Богуш В.М., Юдін О.К. Основи інформаційної безпеки держави: Вступ до спеціальності. Харків: Консум. 439 с.

РОЗДІЛ 7

Методологічні аспекти стратегічного управління діяльністю суб'єктів державного управління у сфері інформаційної безпеки

7.1. Сутність, мета та особливості стратегічного управління забезпеченням інформаційної безпеки

Бурхливий розвиток інформаційних технологій і проблема їх оперативного впровадження в усі сфери життєдіяльності людей, зростання значимості інформації при прийнятті управлінських рішень органами державної влади та управління, новий формат функціонування засобів масової інформації ці та інші чинники виводять на передній план проблему формування та реалізації стратегічного управління забезпеченням інформаційної безпеки.

Захищаючи свої національні інтереси, кожна держава повинна піклуватися про свою інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова її соціально-економічної політики, виходячи з пріоритетів національних інтересів і загроз національній безпеці країни. Із правової точки зору вона ґрунтується на принципах правової демократичної держави та впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій і програм у відповідності до чинного законодавства. В Україні назріла об'єктивна необхідність у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу і рівню розвитку інформаційних технологій, нормам міжнародного права, але одночасно ефективно захищала б власні українські національні інтереси. Відносини, пов'язані із забезпеченням інформаційної безпеки,

як найважливіші сьогодні для суспільства й держави, вимагають як найшвидшого законодавчого регулювання.

Стратегічне управління полягає в умінні моделювати ситуацію; здатності виявляти необхідність змін; розробці самої стратегії; здатності втілювати стратегію в життя. Поряд із цим, стратегічне управління – це управління, яке спирається на людський потенціал як основу організації, орієнтує виробничу діяльність на запити споживачів, гнучко реагує і проводить своєчасні зміни в організації, що відповідають виклику з боку оточення та дають змогу домагатися конкурентних переваг, що в сукупності дає можливість організації виживати в довгостроковій перспективі, досягаючи при цьому своїх цілей.

Таким чином, стратегічне управління – це передусім безперервний процес, а не одноразовий акт із розробки стабільного стратегічного плану. Він починається з оцінки ситуації ззовні й усередині організації, вироблення можливих напрямів застосування сил організації, вибору найкращої з виявлених альтернатив і розробки докладного тактичного плану, направленого на поетапну реалізацію вибраної стратегії [1].

Проведення стратегічного управління забезпечення інформаційної безпеки може істотно вплинути на рішення внутрішньополітичних, зовнішньополітичних та військових конфліктів. Інформаційна безпека є однією з суттєвих складових національної безпеки країни. Її забезпечення завдяки послідовній реалізації грамотно сформульованої державної інформаційної політики значною мірою сприяло б забезпеченню досягнення успіху при вирішенні задач у політичній, соціальній, економічній та інших сферах державної діяльності [2].

Під державною інформаційною політикою необхідно розуміти політику, що засобами державної (політичної) влади створює і забезпечує функціонування системи правового регулювання інформаційних відносин, захист прав і основних свобод людини, збалансованість інтересів людини, суспільства й держави у всіх сферах інформаційної діяльності [3]. Розробка

державної інформаційної політики в Україні повинна передбачати те, що всі проблеми, пов'язані із забезпеченням інформаційної безпеки (формування інформаційного законодавства, протидія загрозам в інформаційній сфері, протидія конфліктам інформаційного характеру, інформаційним війнам, розробка правових засобів і організаційних заходів захисту від інформаційних війн), повинні вирішуватися комплексно [4]. Отже, відзначимо важливість розробки належної, послідовної державної інформаційної політики, спрямованої на отримання якісно нового результату у сфері забезпечення інформаційної безпеки людини, суспільства й держави, яке б відповідало стану й тенденціям розвитку світового інформаційного суспільства та загальновизнаним міжнародним і європейським стандартам у досліджуваній сфері.

У рамках реалізації державної інформаційної політики повинні бути закладені основи для вирішення таких завдань, як-от:

1) формування єдиного інформаційного простору України та її входження до світового інформаційного простору;

2) забезпечення інформаційної безпеки особистості, суспільства й держави;

3) формування демократично орієнтованої масової свідомості;

4) розвиток галузі інформаційних послуг;

5) розширення правового поля регулювання суспільних відносин, у тому числі пов'язаних з отриманням, розповсюдженням і використанням інформації, що, у свою чергу, має сприяти зміцненню зв'язків центру та регіонів, зміцненню цілісності країни.

Ці основи дозволяють сформувати стратегічну мету державної інформаційної політики забезпечення переходу до нового етапу розвитку України, побудова інформаційного суспільства і входження країни до світового інформаційного співтовариства. При цьому мають бути передбачені наступні складові:

– формування й розвиток відкритого інформаційного простору держави при необхідній умові забезпечення її цілісності та єдності;

– інтеграція у світовий інформаційний простір із урахуванням національних інтересів та особливостей;

– забезпечення інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

Успіх державної інформаційної політики буде залежати від виконання наступних першочергових завдань:

– модернізація інформаційно-телекомунікаційної інфраструктури, розвиток інформаційних і телекомунікаційних технологій;

– ефективне формування і використання національних інформаційних ресурсів та забезпечення широкого, вільного до забезпечення громадян суспільно значущою інформацією;

– створення необхідної нормативно-правової бази побудови сучасного інформаційного суспільства.

Виконання вказаних завдань має супроводжуватися належним фунціоналом:

– забезпечення інформаційного обслуговування населення на основі розвитку масового інформаційного обміну та масових комунікацій;

– інформаційне забезпечення діяльності системи органів державної влади й місцевого самоврядування;

– забезпечення інформаційної взаємодії громадянського суспільства і влади, включаючи державну й місцеву владу;

– підготовка людини до життя та роботи в інформаційному суспільстві.

Задля виконання поставлених завдань потрібно регулювання за допомогою різних форм впливу об'єктів інформаційної сфери [5,6], що задіяні в цьому процесі, а саме:

– правова база інформаційних відносин;

– система формування і використання інформаційних ресурсів;

– інформаційно-телекомунікаційна інфраструктура;

– науково-технічний і виробничий потенціал, необхідний для формування інформаційно-телекомунікаційного простору;

– ринок інформаційних і телекомунікаційних засобів, інформаційних продуктів і послуг;

– домашня комп'ютеризація;

– міжнародне співробітництво;

– система забезпечення інформаційної безпеки.

Слід зазначити, що при реалізації завдань державної інформаційної політики мають бути дотримані наступні базові принципи (рис. 7.1.).

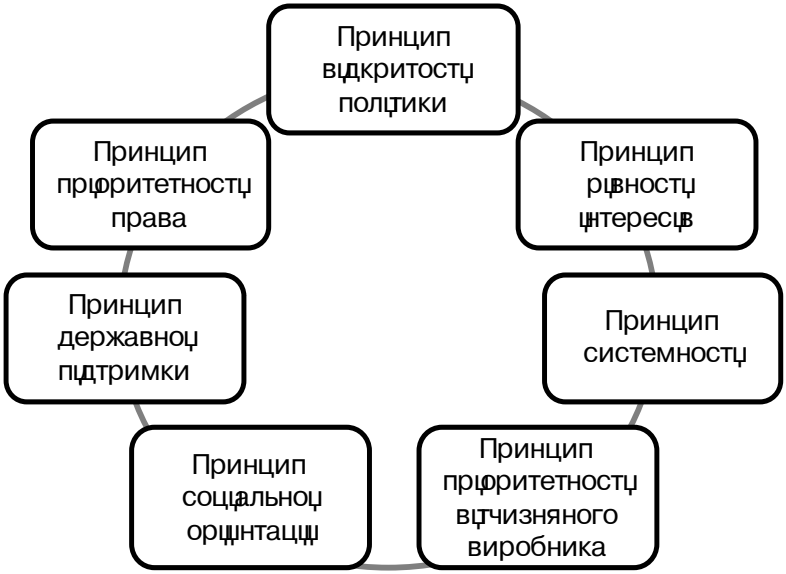


Рис. 7.1. Базові принципи реалізації завдань державної інформаційної політики

Принцип відкритості політики – усі основні заходи інформаційної політики відкрито обговорюються суспільством, і держава враховує громадську думку.

Принцип рівності інтересів – у рівній мірі враховуються інтереси всіх учасників інформаційної діяльності незалежно від їх положення в суспільстві, форми власності та державної приналежності.

Принцип системності – при реалізації прийнятих рішень щодо зміни стану одного з об'єктів регулювання повинні в сукупності враховуватися наслідки цих рішень на стан інших.

Принцип пріоритетності вітчизняного виробника – за рівних умов пріоритет віддається вітчизняному виробникові інформаційно-комунікаційних засобів, продуктів і послуг.

Принцип соціальної орієнтації – основні заходи державної інформаційної політики повинні бути спрямовані на забезпечення соціальних інтересів громадян України.

Принцип державної підтримки – заходи інформаційної політики, спрямовані на інформаційний розвиток соціальної сфери, фінансуються переважно державою.

Принцип пріоритетності права – розвиток і застосування правових і економічних методів має пріоритет перед будь-якими формами адміністративних рішень проблем інформаційної сфери.

Реалізація інформаційної політики включає ключовий набір взаємозв'язаних компонентів (рис. 7.2.).

Рис. 7.2. Компоненти реалізації інформаційної політики

Нормативно-правовий компонент уміщує певний правовий інструментарій, який буде застосований для подолання цих загроз із обов'язковим пріоритетом прав і свобод людини й громадянина, формує певний вектор розвитку інформаційних відносин.

Організаційно-технологічний компонент представлено комплексом організаційних і технологічних засобів пошуку, збереження, розповсюдження та використання інформаційної продукції й послуг в усіх сферах життєдіяльності суспільства й держави, що включає територіально розподілені депозитарії інформаційних ресурсів, державні й корпоративні комп'ютерні мережі, телекомунікаційні мережі та системи спеціального призначення й загального користування, лінії зв'язку, мережі та канали передачі даних, засоби комутації й управління інформаційними потоками, організаційні структури управління й контролю.

Економічний компонент – збереження, розвиток та ефективне використання об'єктів національного інформаційного простору, які мають стратегічне значення для економіки та безпеки України; забезпечення всебічної підтримки й захисту вітчизняного виробника інформаційного продукту, сприяння виробленню і впровадженню новітніх інформаційних технологій; економічна підтримка державою розвитку інформаційної інфраструктури й інформаційної системи, сприяння розробці та впровадженню новітніх інформаційних технологій.

Соціальний компонент – у державі має бути достатня кількість професійно підготовлених спеціалістів для роботи в інформаційних сферах влади та громадянського суспільства, які здатні були б забезпечувати засвоєння, упровадження й ефективну експлуатацію сучасних інформаційних і комунікаційних технологій, систем, мереж і технічних пристроїв, а всі громадяни мають бути досить підготовлені для того, щоб стати їхніми масовими індивідуальними користувачами як у своїй професійній діяльності, так і в домашніх умовах. При цьому і фахівці-професіонали, і масові користувачі повинні добре знати й чітко дотриму-

ватися правових норм діяльності в інформаційній сфері. Важливим соціально-освітнім фактором державної інформаційної політики є формування та розвиток єдиної загальнодержавної системи масової інформаційної освіти й просвіти, підготовки та перепідготовки професійних кадрів інформаційної сфери.

Зважаючи на зростання кількості випадків незаконного застосування інформаційної зброї, несанкціонованого поширення й отримання інформації за допомогою мережі Інтернет, поширення кіберзлочинності, особливої актуальності й значущості набуває процес формування інформаційної політики в електронно-інформаційному середовищі, під яким необхідно розуміти не тільки правові норми, а й загальновизнані моральні канони поведінки, тобто специфічні правила інформаційної культури, нехтування якими негативним чином відображається на реалізації вимог інформаційного законодавства (у тому числі й законодавства у сфері забезпечення державної інформаційної політики та інформаційної безпеки).

Беззаперечно, належний рівень державної інформаційної політики та інформаційної безпеки в державі може бути забезпечений лише за умови створення й ефективного функціонування добре розвиненого інформаційного суспільства. Однак на сьогоднішній день можна визначити ряд недоліків, що заважають його побудові та перешкоджають забезпеченню належного рівня інформаційної безпеки людини, суспільства й держави [7]:

– недостатній розвиток нормативно-правової бази забезпечення належного функціонування інформаційної сфери, забезпечення інформаційної безпеки людини, суспільства й держави – неузгодженість окремих норм законодавства, що регулюють інформаційну сферу;

– недієва система державного регулювання медіапростору, відсутність єдиного бачення напрямків його подальшого розвитку;

– недостатня інформаційна присутність України в глобальному медіа просторі, підвищена інформаційна залежність від іноземних держав і медіаструктури;

– незадовільний стан мережі радіомовлення; застаріле технологічне обладнання українських телерадіокомпаній, недостатній рівень розвитку новітніх засобів комунікації;

– монополізм кабельного мовлення; надзвичайно повільний перехід на цифровий формат мовлення;

– ринкова стихійність телекомунікаційних мереж та комп'ютеризації, низька керованість ними з боку держави;

– нерегульованість підготовки та працевлаштування в межах держави ІТ-фахівців;

– недостатня кількість державних програм, що стосуються формування інформаційного суспільства;

– низький рівень комп'ютерної та інформаційної грамотності населення, повільність упровадження новітніх методів навчання із застосуванням сучасних інформаційно-комунікаційних технологій;

– нерівномірність забезпечення можливості доступу населення до комп'ютерних і телекомунікаційних засобів, поглиблення «інформаційної нерівності» між окремими регіонами, галузями економіки та різними верствами населення;

– низький рівень надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг із використанням мережі Інтернет, низькі темпи розробки відповідної інформаційної інфраструктури;

– низька розробленість механізму захисту авторських прав на комп'ютерні програми, відсутність відповідних системних державних рішень;

– відсутність ефективного захисту інформаційних прав громадян, насамперед, щодо доступності інформації, захисту інформації й мінімізації ризику «інформаційної нерівності» та інші [8, 9].

Державна інформаційна політика повинна враховувати вказані недоліки при плануванні заходів щодо стимулювання розвитку інформаційного суспільства.

На сьогодні в Україні законодавчо сформульовані й закріплені основні принципи, завдання та стратегічні напрями державної інформаційної політики, сформовані державні інститути відповідної компетенції, прийнятий цілий ряд концепцій, програм і планів дій [10]. Однак на рівні практичної реалізації інформаційна політика держави в сучасній Україні відзначається нескоординованістю діяльності різних відомств, непослідовністю й непрозорістю в реалізації намічених заходів. Як наслідок Україна поки що не належить до числа інформаційно незалежних держав, а її інформаційну сферу характеризують такі ознаки:

– малоефективна система державного регулювання національного медіапростору, відсутність консолідованого бачення напрямків його подальшого розвитку, нерозвиненість культурних індустрій, національної системи збору та поширення інформації в глобальному масштабі;

– низький рівень присутності в глобальному медіапросторі, висока інформаційна залежність від іноземних держав і медіаструктури;

– за наявності позитивної динаміки впровадження телекомунікаційних мереж та комп'ютеризації ринкова стихійність цих процесів, низька керованість ними з боку держави, збереження відставання в сфері ІКТ, неврегульованість підготовки та працевлаштування в межах держави ІТ-фахівців.

Державна інформаційна політика повинна реалізовуватися поетапно на основі використання організаційних, правових і економічних механізмів. Передбачається, що реалізація триватиме досить довгий період, строки якого пов'язані з певним рівнем розвитку української економіки. Швидкість цього розвитку визначає зростання потреб в інформації. На першому етапі реалізації державної інформаційної політики слід послідовно

реформувати інформаційне виробництво в системі державної влади та управління в цілому, на другому поступово перетворити наявні інформаційні ресурси в реальні матеріальні й духовні блага для населення країни.

7.2. Інформаційна безпека органів державної влади як основа національної безпеки

У сучасному суспільстві всі сфери життя функціонують на основі розвинутої інформаційної структури. Економічна, політична та військова потужність будь-якої держави в сучасному світі прямо залежить від національного інформаційного ресурсу. Інформація, проникаючи до всіх сфер діяльності держави, набуває конкретного політичного, матеріального і вартісного вираження, що визначається рядом факторів, у тому числі й розмірами заподіяної шкоди, викликаної зниженням її якості.

Безпека інформаційного контенту є одним із основних показників якості такої інформації. Саме тому інформаційна безпека та способи її забезпечення в останні роки набули особливої актуальності в процесі державного управління. Забезпечення інформаційної безпеки органів державної влади розглядається як одне з пріоритетних державних завдань, як важливий елемент національної безпеки. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Роль конкретного органу державної влади в системі забезпечення інформаційної безпеки України визначається місцем у державному механізмі України. Для забезпечення виконання покладених завдань кожен із них наділений відповідними повноваженнями, що включають чітко визначені обов'язки та права [11].

Провідне місце в системі органів державної влади у сфері національної інформаційної безпеки має парламент – Верховна Рада України. Як суб'єкт системи забезпечення інформаційної безпеки вона визначає пріоритети в захисті життєво важливих інтересів об'єктів безпеки, розробляє систему правового регулювання відносин у сфері безпеки, установлює порядок організації й діяльності органів забезпечення безпеки.

Верховна Рада України (ВРУ) здійснює свої функції через законодавче регулювання й контроль за діяльністю органів державної виконавчої та судової влади, їх посадових осіб щодо виконання ними функцій і завдань у сфері національної інформаційної безпеки.

Відповідно до п.5 ст. 85 Конституції України [12] до повноважень ВРУ належить визначення засад внутрішньої і зовнішньої політики держави. Виходячи з цих міркувань, формування державної політики в інформаційній сфері суспільних відносин, їхня безпека є виключно прерогативою парламенту України.

Однією з форм контрольної функції підтримки національної інформаційної безпеки є проведення парламентських слухань, наприклад, із питань свободи слова та інформаційної безпеки України. Таку діяльність парламенту можна розглядати і як координуючу функцію державного управління щодо підтримки правового режиму національної інформаційної безпеки. Призначаючи половину складу (чотирьох осіб) Національної Ради України з питань телебачення й радіомовлення, парламент реалізовує свою контрольну функцію.

Окремими структурами ВРУ, що інтегруються із завданнями національної інформаційної безпеки, є:

• Профільний парламентський Комітет із питань свободи слова та інформації;

• Комітет із питань будівництва, транспорту та зв'язку;

• Інформаційне управління, у складі якого діє прес-служба Верховної Ради;

• Управління комп'ютеризованих систем, де формується парламентська система інформаційно-аналітичного забезпечення (СІАЗ) діяльності всіх структур Верховної Ради України [13].

Інтегруючим елементом системи органів державної влади, зокрема і в інформаційній сфері, є Президент України. У межах своїх повноважень він здійснює керівництво інформаційною сферою України: створює, реорганізує та ліквідує органи виконавчої влади, визначає їхні функції та основні завдання; видає укази й розпорядження, що стосуються функціонування та розвитку національної інформаційної сфери тощо.

Відповідно до п.17 ст.106 Конституції України Президент «здійснює керівництво у сферах національної безпеки й оборони України». На підставі цього Президент здійснює керівництво у сфері інформаційної безпеки держави, у тому числі у сфері забезпечення інформаційного суверенітету та національної безпеки як важливих складових національної безпеки. Він створює, реорганізовує та ліквідовує окремі органи виконавчої влади, визначає їхні функції та основні завдання. Правовою формою реалізації волі Президента України є укази та розпорядження, у тому числі й ті, що стосуються функціонування та розвитку інформаційної сфери.

Згідно з ч.3. ст.106 Конституції України, Президент видає укази й розпорядження, що є обов'язковими до виконання на території України. Це право Президента широко ним використовується для регулювання питань, пов'язаних із функціонуванням інформаційної сфери.

Слід зазначити, що відповідно до п.1 ст.106 Конституції України, Президент України забезпечує національну безпеку держави. Тоді як повноваження Верховної Ради в цій сфері характеризуються словом «визначає» (п.17 ст.92 Конституції).

У взаємовідносинах із ВРУ Президент України має часткові повноваження щодо формування державних органів в окремих сферах суспільних інформаційних відносин. За приклад можна

навести призначення половини складу (чотирьох осіб) Національної Ради України з питань телебачення й радіомовлення.

Окрім цього, проаналізувавши положення чинних нормативно-правових актів, можна дійти висновку, що Президент України:

– забезпечує взаємодію всіх гілок державної влади між собою, а також із недержавною складовою системи забезпечення національної безпеки в інформаційній сфері;

– видає нормативно-правові акти з питань забезпечення національної безпеки в інформаційній сфері;

– визначає реальні, потенційні загрози й небезпеки для національної безпеки в інформаційній сфері та вживає необхідних заходів із її забезпечення.

Серед координуючих органів державної влади на найвищому рівні державного управління особлива роль відводиться Раді національної безпеки й оборони України (далі РНБО України). РНБО України, яку очолює глава держави, координує та контролює діяльність органів виконавчої влади у сфері національної інформаційної безпеки.

РНБО України подає на розгляд глави держави пропозиції з таких питань: визначення стратегічних національних інтересів України в інформаційній сфері, концептуальних підходів та напрямків збереження національної інформаційної безпеки; доцільність утворення, реорганізації та ліквідації органів виконавчої влади в інформаційній сфері; проєкт державного бюджету за статтями, що пов'язані з підтримкою на належному рівні національної інформаційної безпеки; заходи інформаційного та іншого змісту відповідно до масштабу потенційних та реальних загроз національним інтересам України.

Найважливішим елементом, що забезпечує реалізацію зусиль усіх державних і суспільних сил країни стосовно забезпечення інформаційної безпеки, виступає її система виконавчої влади. Розрізняють наступні види органів виконавчої влади, що розташовані на різних структурних рівнях цієї системи.

Кабінет Міністрів України – вищий орган у системі виконавчої влади (ч. 1 ст.113 Конституції України). Конституцією України закріплені широкі повноваження Кабінету Міністрів України у сфері інформаційних відносин, які визначені нормами ст. 116 Конституції України, зокрема: забезпечення проведення державної інформаційної політики (п.п. 1 та 3), ужиття заходів щодо захисту інформаційних прав і свобод громадян (п. 2), розробка та здійснення загальнодержавних програм щодо розвитку інформаційної сфери (п. 4), передбачення при формуванні державного бюджету коштів на різного роду заходи щодо забезпечення інформаційної безпеки (п. 6), загальна координація діяльності органів виконавчої влади щодо захисту інформаційної безпеки (п. 9) тощо.

Здійснення стратегічного, оперативного й повсякденного державного управління в окремих галузях і секторах народного господарства покладено на центральні органи виконавчої влади (ЦОВВ). Кількість та перелік ЦОВВ законодавчо не закріплені, що характерно для більшості демократичних країн. Адже об'єктивно існуючі завдання держави, що визначають її функції, вирішальним чином упливають на організаційну структуру ЦОВВ, яка, відповідно до функціональних трансформацій, є змінною. Саме тому в Україні їхня кількість, перелік, завдання та функції встановлюються указами глави держави.

Провідне місце серед центральних органів посідають міністерства України. Їхні керівники – міністри – входять до складу Кабінету Міністрів і безпосередньо беруть участь у формуванні державної політики в країні. Міністри особисто відповідають за розробку і впровадження програм Кабінету Міністрів, зокрема щодо інформаційного забезпечення безпеки держави.

До ЦОВВ зі спеціальним статусом, які наділені загальними та спеціальними повноваженнями у сфері інформаційного забезпечення системи органів державного управління, належать:

– Антимонопольний комітет України;

– Державний комітет телебачення й радіомовлення України;

– Фонд державного майна України.

Спеціальні повноваження в інформаційній сфері надано Державному комітету телебачення й радіомовлення України. Держкомтелерадіо України є спеціально уповноваженим центральним органом виконавчої влади із забезпечення реалізації державної політики в інформаційній та видавничій сферах, державної мовної політики.

Спеціальними повноваженнями в інформаційній сфері наділена Служба безпеки України (СБУ) та Служба зовнішньої розвідки України (СЗРУ) [14,15]. СБУ виконує одну з головних функцій, а саме реалізацію державної політики щодо захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації.

На СЗРУ із метою забезпечення інформаційної безпеки держави покладаються такі основні завдання: здійснення спеціальних заходів упливу, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, військово-технічній, екологічній та інформаційній сферах, зміцнення обороноздатності, економічного й науково-технічного розвитку; ужиття заходів протидії зовнішнім загрозам національній безпеці України, життю, здоров'ю її громадян та об'єктам державної власності за межами України.

Відповідно до Конституції України найнижчим рівнем системи органів виконавчої влади є місцеві державні адміністрації, які також здійснюють ряд функцій у сфері забезпечення інформаційної безпеки (наприклад, здійснення заходів щодо організації правового інформування та інформаційного виховання населення; здійснення передбачених законодавством заходів, пов'язаних із забезпеченням інформаційної безпеки, захистом інформаційних прав особи тощо).

В умовах формування інформаційного суспільства важливого значення набуває функціонування громадських організацій як суб'єктів системи забезпечення інформаційної безпеки. Активна діяльність громадських структур в інформаційній

сфері, по-перше, забезпечує участь громадськості в прийнятті рішень із питань інформаційної безпеки, що робить можливим урахування інтересів широких верств населення і тим самим створення засад легітимності рішень органів публічної влади у сфері безпеки. По-друге, введення інститутів громадянського суспільства в механізм політики інформаційної безпеки забезпечує процес залучення громадян у вирішенні проблем інформаційної безпеки, їхню активну позицію з відповідних питань. І, нарешті, наявність недержавних суб'єктів забезпечує відкритість відповідних органів публічної влади та створення дієвих механізмів громадського контролю їхньої діяльності. Це створює основи для втілення в життя таких важливих принципів: пріоритету прав людини; демократичного цивільного контролю за воєнною сферою, а також іншими структурами в системі безпеки; додержання балансу інтересів особи, суспільства та держави, їхньої взаємної відповідальності [11].

Згідно з Доктриною інформаційної безпеки України (далі – Доктрина), інформаційна безпека є самостійною сферою забезпечення національної безпеки України й одночасно невід'ємною складовою кожної з її сфер [16].

Доктрина визначає:

– принципи забезпечення інформаційної безпеки України;

– життєво важливі інтереси в інформаційній сфері України в контексті інтересів особистості, суспільства, держави;

– реальні й потенційні загрози інформаційній безпеці України у сфері державної безпеки та в зовнішньополітичній, військовій, внутрішньополітичній, економічній, соціальній, гуманітарній, науково-технологічній, екологічній сферах.

Ефективність викладених у Доктрині положень залежатиме від ретельності, послідовності, вчасності, якості їхнього виконання, а також інших чинників, що впливатимуть на реалізацію в цілому державної політики в інформаційній сфері на всіх рівнях усіма суб'єктами інформаційних відносин.

Діяльність органів державної влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства й людини за трьома головними напрямками: інформаційно-психологічному, технологічного розвитку та захисту інформації [17].

Інформаційно-психологічний напрямок гарантує забезпечення конституційних прав і свобод людини, сприяє утвердженню загальнолюдських і національних моральних цінностей в інформаційному просторі (дерегуляція, демонополізація, захист свободи слова, реформа медіапростору, гармонізація із європейським законодавством).

Технологічний розвиток відповідає за впровадження новітніх телекомунікаційних технологій та сприяє зростанню інформаційних ресурсів, створенню системи державних стратегічних комунікацій, комунікативній підтримці проведення реформ, реформі урядових комунікацій. У свою чергу захист інформації забезпечує конфіденційність, цілісність та доступність до неї.

Для реалізації зазначеного доцільно звернути увагу на життєво важливі інтереси, що достатньо ґрунтовно представлено в роботі О. Сосніна [18]. Він указує, що національні інтереси в інформаційній сфері – визнана державою збалансована сукупність соціальних інтересів особистості, суспільства й держави, реалізованих в інформаційній сфері, включаючи їхні інтереси в збереженні національної ідентичності. Ураховуючи це, нами було визначено:

1. Інтереси особистості: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання у зміст, процеси обробки, передачі і використання персональних даних, а також у захисті інформації, що забезпечує особисту безпеку захищеність від негативного інформаційно-психологічного впливу, підтримку певного правового статусу людини й громадянина в інформаційній сфері;

2. Інтереси суспільства: збереження та примноження духовних, культурних і моральних цінностей Українського народу; забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формування й розвиток демократичних інститутів громадянського суспільства; захист українського суспільства від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету й територіальної цілісності України, використання інформаційної інфраструктури для розвитку всіх сфер громадського життя;

3. Інтереси держави: недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав і міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; побудова й розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір, використання інформаційної інфраструктури для забезпечення державної політики, управління справами суспільства, захисту моральних цінностей суспільства, а також забезпечення стійкого функціонування інформаційної інфраструктури.

Інформаційна безпека нерозривно пов'язана з інформаційною безпекою самих державних органів, адже вони виступають суб'єктами забезпечення інформаційної безпеки, використовуючи технологічні, правові, організаційні засоби.

До інформаційної безпеки органів державної влади можна віднести наступні ключові складові:

• забезпечення їх інформаційних потреб у рамках їх компетенції і в обсягах, необхідних для виконання покладених на них завдань, повноту, своєчасність і достовірність інформації, необхідної для прийняття рішень;

• безпеку інформації та інформаційних ресурсів;

• безпеку телекомунікацій та інформаційного обміну.

Інформаційне забезпечення діяльності органів державної влади – неодмінна умова ефективності державного управління, прийняття обґрунтованих рішень на основі повної, своєчасної та достовірної інформації. Рівень інформаційного забезпечення діяльності органів державної влади має суттєвий вплив на всі процеси соціально-економічного розвитку суспільства, є одним із стратегічних напрямків підвищення ефективності діяльності на всіх рівнях.

Необхідні оцінка й забезпечення інформаційних потреб у рамках кожної функції управління конкретного органу державної влади; організація документообігу та обміну інформацією; оптимізація потоків інформації і процедур обміну тощо. Обсягу компетенції кожного органу державної влади повинен відповідати необхідний для її реалізації обсяг інформаційного забезпечення, при цьому на інформаційну безпеку буде мати негативний вплив як недолік інформації, так і її надлишок. Це призводить до необхідності визначати обсяг інформаційного забезпечення конкретного органу державної влади в положенні про цей орган, іншими словами, установлювати його інформаційний статус на основі поставлених перед ним завдань і обсягів наданих повноважень.

На підвищення інформаційної безпеки органів державної влади впливає створення на національному й регіональному рівнях електронного уряду з урахуванням новітніх інформаційно-комунікаційних технологій, у результаті чого забезпечується сучасна інформаційна основа для прийняття управлінських рішень, підвищується рівень інформаційного забезпечення, достовірність, швидкість отримання та повнота інформації.

При цьому не можна зводити електронний уряд тільки до його технічної складової; його завдання підвищення ефективності діяльності держави в цілому, формування нового рівня відносин громадян зі своєю державою.

Цілями формування електронного уряду в тому числі є підвищення якості адміністративно-управлінських процесів, удосконалення системи інформаційно-аналітичного забезпечення рішень, які приймаються на всіх рівнях державного управління.

Безпека інформації як складова інформаційної безпеки органів державної влади включає в себе захист інформації та інформаційних ресурсів від несанкціонованого доступу, спотворення, знищення, установлення режиму інформації в залежності від її змісту, забезпечення захисту відомостей, що становлять державну таємницю, іншої інформації обмеженого доступу.

Безпека інформації, що циркулює в органах державної влади, забезпечується різними заходами (рис.7.3.).

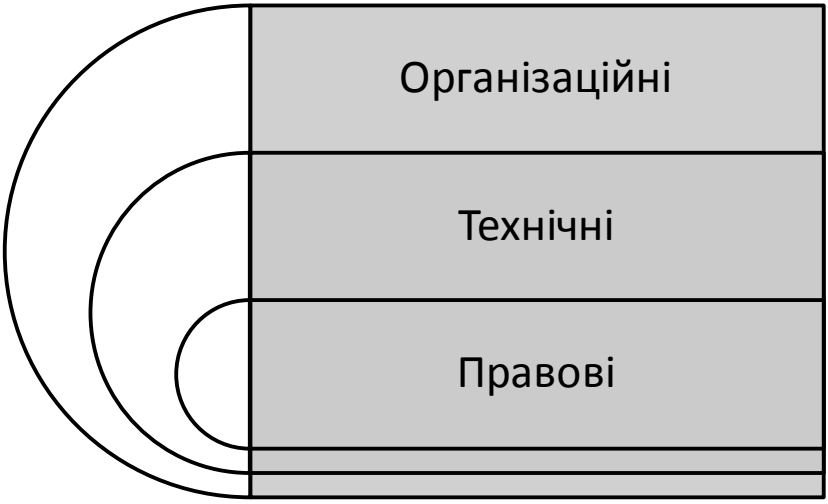


Рис. 7.3. Заходи безпеки інформації в органах державної влади

Організаційні – забезпечення захисту інформації від незаконного втручання, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій стосовно такої інформації;

Технічні – дотримання конфіденційності інформації обмеженого доступу;

Правові – реалізація права на доступ до інформації.

Безпека телекомунікацій та інформаційного обміну – одна зі складових інформаційної безпеки органів державної влади. Інформаційні технології знайшли широке застосування в управлінні найважливішими об'єктами життєзабезпечення, які стають більш уразливими перед випадковими й навмисними діями. Підвищення вразливості пов'язане з цілою низкою чинників, основними з яких є зниження рівня міжнародної безпеки, розвиток міжнародного тероризму, збільшення кількості потенційно небезпечних об'єктів.

Однак наведені вище заходи, безумовно, необхідні, але недостатні. Фактори уразливості в інформаційній сфері України визначаються наявністю таких серйозних проблем: істотна залежність національних інфраструктур від зарубіжних технологій; недостатній рівень захищеності критично важливих сегментів інформаційної інфраструктури; низький ступінь державного контролю її внутрішнього інформаційного простору. Це зумовило виникнення нових загроз, які пов'язані, перш за все, із можливістю використання інформаційно-комунікаційних технологій у цілях, несумісних із національними інтересами.

Неухильне наростання загроз, застосування інформаційних і комунікаційних технологій у військово-політичних, у тому числі в якості інформаційної зброї, терористичних і кримінальних цілях обумовлює необхідність забезпечення інформаційної безпеки держави в цілому та органів державного управління, зокрема на основі не тільки короткострокового (подолання турбулентності й досягнення керованості), але й середньострокового (формування повністю керованої структури й концепції

інформаційної безпеки) та довгострокового (створення умов, щоб Україна стала незалежним гравцем на світовій арені) планування. Воно має здійснюватися на основі комплексного аналізу результатів оцінки функціонування системи інформаційної безпеки органів державної влади з урахуванням динаміки загроз в інформаційній сфері.

Згідно з проєктом Закону України «Про державне стратегічне планування» [19] стратегічне планування в системі інформаційної безпеки органів державної влади можна відобразити відповідно до рис. 7.4.

Рис. 7.4. Стратегічне планування в системі інформаційної безпеки органів державної влади

Цілепокладання – доктрина інформаційної безпеки органів державної влади (визначення цілей, пріоритетів та напрямків забезпечення *інформаційної безпеки органів державної влади*);

Прогнозування – стратегічний прогноз у частині, що стосується інформаційної безпеки органів державної влади (визначення науково-обґрунтованих уявлень про загрози інформаційної безпеки державних органів, уключаючи можливі сценарії їх реалізації і прогнозних оцінок стану інформаційної безпеки органів державної влади);

Планування – національний план удосконалення системи інформаційної безпеки органів державної влади;

Програмування – державні програми органів державної влади, галузеві відомчі програми.

Такий підхід дозволить розробити дієву концепцію системи інформаційної безпеки органів державної влади, яка буде спрямована на підвищення ефективності їхньої діяльності, на захист інтересів особистості, суспільства й держави, і сприятиме:

– зростанню довіри громадян до електронних послуг, які надаються на порталах державних органів;

– зміцненню державних гарантій недоторканності приватного життя при використанні інформаційних і телекомунікаційних технологій;

– посиленню співпраці громадянського суспільства, бізнесу й держави в різних областях (у тому числі з використанням електронних технологій);

– інформаційній підтримці участі громадян в управлінні державою;

– розвитку та впровадженню інформаційних технологій в органах державної влади;

– розвитку послуг зв'язку та обробки інформації, що надаються громадянам, організаціям;

– забезпеченню захисту національних інтересів в інформаційній сфері від внутрішніх і зовнішніх загроз.

Слід зазначити, що формування системи інформаційної безпеки органів державної влади має спиратися на міжнародний досвід інших країн, а також має відбуватися в тісному спів-

робітництві з міжнародними організаціями та форумами. В основу розроблення концепції та доктрин інформаційної протидії більшості провідних західних країн, а також керівних документів НАТО покладені підходи щодо організації та проведення інформаційних операцій, які існують в армії США. Проблеми інформаційної війни у США знаходяться в центрі уваги воєнно-політичного керівництва. Концепція «інформаційної війни» базується на тому, що інформація та інформаційні технології мають дуже важливе значення як для національної безпеки в цілому, так і для військових дій безпосередньо. Практична реалізація Концепції здійснюється шляхом проведення інформаційних операцій, під якими розуміється комплекс заходів, що проводиться за єдиним планом і задумом із метою здійснення впливу на інформацію й інформаційно-управляючі системи противника при одночасному захисті власної інформації та інформаційно-управлінські системи [20].

Отже, як уже зазначалося, забезпечення інформаційної безпеки державного управління, органів державної влади є одним зі стратегічно важливих завдань для зміцнення національної безпеки держави. Розглянуті проблеми відносяться до тих, що вимагають постійної уваги держави та пріоритетного вирішення, підвищення ступеня державного контролю за дотриманням вимог безпеки в інформаційному просторі. Суттєвим внеском у забезпечення інформаційної безпеки може стати розробка концептуальних засад визначення оптимальних шляхів щодо вдосконалення системи інформаційної безпеки України.

7.3. Концептуальні засади визначення оптимальних шляхів щодо вдосконалення системи інформаційної безпеки України

Сучасний стан інформаційної безпеки в Україні стан нового, який оформлюється з урахуванням веління часу. На шляху його розвитку багато вже зроблено, але ще є й багато проблем,

які потребують оновлення теоретичного базису їх вирішення та практичного втілення наукових досягнень. Як зазначалося в попередніх розділах, за останні роки проведено ряд заходів щодо вдосконалення інформаційної безпеки:

– По-перше, розпочато розвиток бази правового забезпечення інформаційної безпеки. Було затверджено ряд законів, що регулюють суспільні відносини в цій сфері, сформована робота щодо створення механізмів їхньої реалізації;

– По-друге, на поточний момент проведені першочергові заходи щодо забезпечення інформаційної безпеки в органах державної влади, на підприємствах, в організаціях та установах незалежно від форм власності. Розгорнуто діяльність зі створення захищеної інформаційно-телекомунікаційної системи особливого призначення за участі органів державної влади;

– По-третє, забезпеченню інформаційної безпеки сприяють створені державою системи:

– державна система захисту інформації;

– система ліцензування практики в області захисту державної таємниці;

– система сертифікації методів захисту інформації.

Однак аналіз показує, що все ще існують певні проблеми, що істотно перешкоджають повноцінному забезпеченню інформаційної безпеки людини, суспільства й держави, захисту їхніх прав і свобод в інформаційній сфері. Серед таких, що потребують вирішення, можна виділити:

– розвиток системи забезпечення інформаційної безпеки, яка здійснює єдину державну політику в цій галузі;

– удосконалення нормативно-правової бази забезпечення інформаційної безпеки;

– розвиток науково-практичних основ забезпечення інформаційної безпеки з урахуванням актуальної геополітичної ситуації, умов політичного й соціально-економічного розвитку та можливості загроз застосування інформаційної зброї;

– реалізація сучасних методів і засобів захисту інформації, забезпечення безпеки інформаційних технологій, у першу чергу, у системах управління військами та зброєю, екологічно небезпечними й економічно значущими виробництвами;

– розвиток і вдосконалення систем захисту інформації та державної таємниці;

– розширення взаємодії із зарубіжними й міжнародними органами та організаціями для забезпечення безпеки інформації, що передається за допомогою міжнародних телекомунікаційних систем і систем зв'язку [21].

Удосконалення організаційно-функціонального забезпечення державного управління у сфері інформаційної безпеки України покликано сприяти уникненню дублювання функцій державного управління, посиленню контролю та відповідальності з боку держави й громадськості в цій сфері, адаптації механізму формування та реалізації державної безпекової й інформаційної політики до передових світових практик. Вони передбачають наближення влади до населення, публічність процесу прийняття управлінських рішень, що дає можливість зробити більш точним його аналіз із метою коригування й оптимізації своєї роботи; викликає в громадськості відчуття причетності до творення та реалізації політики; населення починає сприймати її як партнера, помічника, а не як щось відокремлене та вороже, тим самим забезпечуючи інформаційну безпеку в державі [22-24]. Це може допомогти більш чіткому визначенню основних функцій і завдань органів державної влади в центрі та регіонах під час її забезпечення й організації процесу залучення громадськості. Для цього необхідно розробити й реалізувати державну довгострокову програму створення основ інформаційного суспільства, яка може стати об'єднуючим ідейним початком для України, оскільки поряд із концепцією моделі стійкого її розвитку дає цільову спрямованість суспільного розвитку, і на цій основі можуть бути визначені конкретні шляхи досягнення цілей, пов'язаних з інформаційною безпекою України.

Також удосконалення потребує організаційно-функціональне забезпечення роботи Міністерства інформаційної політики України. Для поступового переходу України на новий етап розвитку необхідно забезпечити умову, за якої її загальнодержавні інтереси будуть невід'ємною складовою частиною інтересів регіонального інформаційного співтовариства. Це можливо, насамперед, за умови дієвої децентралізації повноважень і міжінституційної взаємодії – центральних і регіональних державних органів (загальної та спеціальної компетенції), тобто шляхом узгодження їхніх напрямків діяльності у сфері інформаційної безпеки. Реалізація їхніх можливостей – питання адекватної політики і своєчасних публічно-управлінських рішень. Для цього Міністерство інформаційної політики України, як інші ЦОВВ, що виконують специфічні функції державного управління в окремій сфері та галузі економіки, повинно мати розгалужену, ієрархізовану та найбільш наближену до об'єкта впливу організаційну будову. Ідеться, з одного боку, про вдосконалення основної організаційної будови Міністерства інформаційної політки України, тобто про необхідність створення регіональних структурних підрозділів і представництв як оперативного ядра, найбільш наближеного до вияву та нейтралізації загроз інформаційній безпеці України на регіональному рівні. А з іншого боку, про вдосконалення функціонально-допоміжної організаційної будови Міністерства інформаційної політки України, тобто про необхідність створення регіональних громадських рад при структурних його регіональних представництвах.

Із огляду на той факт, що інформація й новітні інформаційно-телекомунікаційні технології все більше визначають розвиток держави й суспільства, їх інтенсивне впровадження в усі сфери суспільного життя, у тому числі й широке застосування в управлінні державою, особливої актуальності та значущості набуває розробка й реалізація концептуальних основ державної інформаційної політики, у тому числі належне забезпечення інформаційної безпеки на законодавчому рівні. Обов'язок за-

безпечення інформаційної безпеки покладається на всіх суб'єктів, що функціонують в інформаційній сфері, але ключову роль у проведенні інформаційної політики має відігравати держава в особі відповідних органів державної влади. Забезпечення інформаційної безпеки з боку держави має реалізовуватися шляхом розробки нормативно-правових актів, спрямованих на формування узгодженої державної інформаційної політики, концепцій і програм розвитку та модернізації сектора інформаційної безпеки, належне забезпечення інформаційної безпеки та виведення зазначеної діяльності на якісно новий рівень [25].

Дослідження основних положень нормативно-правових актів, що регулюють сферу державної інформаційної політики та інформаційної безпеки, дозволяє зробити висновок, що одним із пріоритетів розвитку національного інформаційного законодавства є створення цілісної системи законодавства з питань розвитку інформаційного суспільства та забезпечення інформаційної безпеки, у тому числі здійснення кодифікації інформаційного законодавства. Необхідність розробки Інформаційного кодексу обумовлена наступними факторами: наявністю значного масиву нормативно-правових актів, що регламентують суспільні інформаційні відносини й забезпечують інформаційну безпеку; не всі зазначені нормативно-правові акти пов'язані між собою, спостерігається їх концептуальна й термінологічна неузгодженість, діють застарілі та неефективні норми. Такий стан справ вимагає серйозного переосмислення підходів до законодавчого врегулювання питань забезпечення інформаційної політики та безпеки, захисту прав на інформацію, формуванню єдиної структури системи правових норм у системі інформаційного законодавства (у тому числі й із питань забезпечення інформаційної безпеки), гармонізації з європейськими та іншими міжнародними стандартами.

Вважаємо за необхідне акцентувати увагу на тому, що проблема практичної розробки дієвого Інформаційного кодексу України, положення якого враховували б міжнародні та євро-

пейські стандарти у сфері захисту інформації та забезпечення інформаційної безпеки, є надзвичайно важливим і складним завданням. Підкреслимо, що розробка кодексу має відбуватися з урахуванням принципів справедливості, державних гарантій, охорони й захисту загальновизнаних прав людини на інформацію в інформаційному просторі суспільства.

При вирішенні значущих завдань і реалізації першочергових заходів державної політики щодо забезпечення інформаційної безпеки на сьогоднішній день переважає прагнення вирішувати переважним чином нормативно-правові та технічні проблеми.

Для формування системи інформаційної безпеки слід розробити і встановити політику інформаційної безпеки, яку необхідно погоджувати з наявними законами та правилами, які стосуються організації, а саме ці закони та правила необхідно виявляти і враховувати при розробці політики.

Із урахуванням сучасного стану інформаційної сфери України першочерговими завданнями інформаційної політики держави повинні стати:

1) створення потужної і конкурентоспроможної національної системи інформаційного виробництва, здатної забезпечити консолідацію суспільства на основі спільних цінностей, завдань, ідей, що сприяє всебічному розвитку особистості;

2) подальша технологічна модернізація з орієнтацією на розширення присутності в міжнародному поділі праці у сфері інформаційно-комунікаційних технологій.

Перспективними шляхами подолання проблем, ефективного забезпечення та вдосконалення системи державної інформаційної політики та інформаційної безпеки (у тому числі протидії інформаційним війнам) можна вважати:

1) удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, у тому числі захисту інформаційних ресурсів, протидії інформаційним війнам, протидії комп'ютерній злочинності, захисту персональних даних;

2) концентрацію діяльності органів державної влади й ресурсів держави на пріоритетних завданнях розвитку інформаційного суспільства та забезпечення інформаційної безпеки;

3) підвищення рівня координації діяльності органів державної влади щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення ефективного міжнародного співробітництва з цих питань;

4) запровадження міжвідомчого підходу та ієрархічності в організації системи забезпечення інформаційної безпеки держави. Її організація та структура повинна відповідати існуючій структурі державного управління з чіткою координацією дій окремих сегментів;

5) організація ефективної системи забезпечення інформаційної безпеки потребує централізованого управління із конкретними відомчо-розпорядницькими функціями, які забезпечують моніторинг і контроль за всіма складовими національного інформаційного простору. Система забезпечення інформаційної безпеки має за будь-яких ситуацій володіти здатністю зберігати необхідні параметри для її функціонування;

6) реалізацію правоохоронної діяльності в інформаційній сфері, тобто організацію діяльності відповідних правоохоронних органів щодо забезпечення інформаційної безпеки (у тому числі протидії інформаційним війнам) на належному рівні відповідно до світових стандартів;

7) сфера кібернетичної безпеки вимагає проведення систематичних тренінгів або навіть навчань суб'єктів протидії кіберзагрозам у разі виникнення таких ситуацій. На цих заходах мають відпрацьовуватися алгоритми типових дій підрозділів Збройних сил України, Національної гвардії України, Служби Безпеки України та інших зацікавлених сторін щодо нейтралізації кібернетичних загроз, усунення факторів, що сприяли їм та притягнення винних до відповідальності;

8) цілеспрямованого впровадження позитивного зарубіжного досвіду організації та проведення інформаційних операцій, форм, методів, засобів здійснення кібератак, а також моделювання інформаційних нападів;

9) створення багатофункціональної інформаційної інфраструктури держави та забезпечення захисту її елементів із метою належного забезпечення інформаційних та майнових прав і свобод громадян потребують систематичного вдосконалення механізмів зберігання, передачі та обробки даних державних реєстрів та баз даних із застосуванням сучасних інформаційно-комунікаційних технологій, приведення їх функціонування у відповідність із міжнародними стандартами.

Підсумовуючи сказане і погоджуючись із концепцією О. Смирнова [26], що Україна – це Земля Нових Можливостей, підкреслимо, що інформаційна безпека – це організм, система, що буде робочою в тому випадку, якщо буде керованою. Очевидно, що інформаційна безпека завжди буде похідною від стратегії розвитку самої держави. Адже саме дії громадян, здійснення їхніх планів і способу життя повинна забезпечувати вдосконалена система інформаційної безпеки.

Список використаних джерел

1. Ковбасюк Ю.В. (голова), К.О. Ващенко (заст. голови), Ю.П. Сурмін (заст. голови) [та ін.]. Державне управління: підручник: у 2 т. Нац. акад. держ. упр. при Президентові України; ред. кол. К.; Дніпропетровськ. НАДУ. 2012. Т. 1. 564 с.

2. Панченко О.А. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. Серія: Державне управління. 2019. Випуск 3. URL: http://77.222.145.174/index.php/governance/article/view/296/297 (дата звернення 10.04.2020).

3. Арістова І.В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики: монографія. Х.: Нац. ун-т внутр. справ. 2006. 354 с.

4. Почепцов Г. Інформаційна політика: навч. посібник. К.: Знання. 2006. 663 с.

5.Степанов В.Ю. Государственная информационная политика: цель и теоретические основы реализации. URL: http://archive.nbuv.gov.ua/portal/soc_gum/Dtr_du/2011_2/files/DU211 (дата звернення 10.05.2020).

6. Панченко О.А. Засоби масової комунікації як платформа державної інформаційної політики. Державне управління: удосконалення та розвиток. Київ. № 4. 2020. DOI: 10.32702/2307-2156-2020.4.2. URL: http://www.dy.nayka.com.ua/pdf/4_2020/4.pdf (дата звернення 10.05.2020).

7. Панченко О.А. Суспільний запит на інформаційну безпеку. Публічне урядування.№ 2 (22).С. 141-149. DOI: 10.32689/2617-2224-2020-2(22)-141-149. URL: https://vadnd.org.ua/app/uploads/2020/05/Публічне-урядування-2-22_укр.pdf (дата звернення 10.05.2020).

8. Старіш О.Г. Інформаційна політика держави в контексті глобалізації. Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.03. Політична культура та ідеологія. Київський національний університет імені Тараса Шевченка. Київ. 2008. 401 с.

9. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: моногр. Заг. ред. Р.А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України. 2014. 196 с.

10. Актуальные проблемы государственной информационной политики в Украине Аналитическая записка. URL: http://old.niss.gov.ua/Monitor/april08/3.html (дата звернення 10.04.2020).

11. Березовська І.Р. Суб'єкти у сфері забезпечення інформаційної безпеки в Україні. Наукові записки Львівського

університету бізнесу та права. 2013. Вип. 10. С. 148-153. URL: http://nbuv.gov.ua/UJRN/Nzlubp_2013_10_35 (дата звернення 13.04.2020).

12. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року. Відомості Верховної Ради України. 1996. №30. Ст. 141.

13. Служба інформаційно-аналітичного забезпечення органів державної влади (СІАЗ). URL: http://www.nbuv.gov.ua/siaz.html (дата звернення 10.04.2020).

14. Про Службу безпеки України: Закон України від 25 березня 1992 р. Відомості Верховної Ради. 1992. №27. Ст. 382.

15. Закон України «Про Службу зовнішньої розвідки України» від 01 грудня 2005 року № 3160. Відомості Верховної Ради України. 2006. № 8. С. 231. Ст. 94.

16. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення 10.04.2020).

17. Коваль З. Проблематика протидії інформаційно-психологічним загрозам Україні засобами державного управління. електрон. наук. фах. вид. 2013. Вип. 13. URL: http://nbuv.gov.ua/j-pdf/tppd_2013_13_12.pdf (дата звернення: 02.04.2020).

18. Соснін О. Національні інтереси в інформаційній сфері. Віче. 2011. № 9. С. 32-36. URL:http://nbuv.gov.ua/UJRN/viche_2011_9_15 (дата звернення: 05.04.2020).

19. Проєкт Закону про державне стратегічне планування від 03 листопада 2011 р. №9407. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=9407&skl=7 (дата звернення 13.04.2020).

20. Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України. Дисертація на здобуття наукового ступеня кандидата наук з державного управління. 25.00.02. Механізми державного

управління. Національна академія державного управління при Президентові України. Київ. 2017. 218 с.

21. Панченко О.А. Турбулентні соціально-психологічні виклики в системі державного управління інформаційною безпекою. Теорія та практика державного управління.2020. Том 1. № 68. С. 210-217. URL: http://tpdu.journal.kharkiv.ua/index.php/tpdu/article/view/159/142 (дата звернення 13.05.2020).

22. Arnstein S. A ladder of citizen participation in the USA. Journal of the Royl Town Planning Institute. 1971. Vol. 57. № 4. pp. 176-182.

23. The Global Information Infrastructure: Agenda for Coohtration /R. Brown, L. Irving, A. Prfbhakar, S. Katzen. 1995. 680 p.

24. Pitter A. Steinbuch. Projekt organization und management auf demGebiet der Informationssicherheit, 1998. № 1. pp. 24-25.

25. Панченко О.А. Проблеми правового забезпечення державного управління інформаційною безпекою. Державне управління: удосконалення та розвиток. Київ. № 11. 2019. DOI: 10.32702/2307-2156-2019.11.3. URL: http://www.dy.nayka.com.ua/?op=1&z=1561 (дата звернення 13.04.2020).

26. Смирнов А. Коммуникационная стратегия информационной безопасности Украины. URL: http://hvylya.net/analytics/politics/kommunikatsionnaya-strategiya-informatsionnoy-bezopasnosti-ukrainyi.html (дата звернення: 23.04.2020).

ВИСНОВКИ

Світові тенденції суспільного розвитку свідчать про настання епохи турбулентності, коли непередбачувано виникають природні, економічні та соціально-політичні проблеми, що супроводжуються нестабільністю та насильством, порушенням внутрішнього соціального порядку в державі та погіршенням міжнародних відносин. Основною ознакою турбулентного стану сучасного суспільства є потокова реальність, і, у силу цього, суспільство пронизане хаотичними, неконтрольованими процесами. За таких умов відбуваються істотні негативні зміни в психічному стані населення, наслідки становлять небезпеку для нормального існування й розвитку держави. Таким чином, забезпечення національної безпеки, де однією з головних є інформаційна складова, виступає важливим моментом у цьому контексті (акцентуація на інформаційно-психологічному аспекті безпеки).

При забезпеченні інформаційно-психологічної безпеки великого значення набуває ціннісний потенціал і актуальні потреби. Зміст аксіологічного бачення інформаційно-психологічної безпеки полягає в забезпеченні психологічного благополуччя особистості з мінімізацією різноманітних ризикових факторів формування і функціонування адекватної інформаційно-орієнтовної основи суб'єктивно-особистісних відносин до навколишнього світу і самої себе. Модернізована піраміда людських потреб відповідно до сучасних трансформацій інформаційного суспільства, динамізму структури бажань і потягів представляє ієрархічну структуру соціальної поведінки людини як основи інформаційно-психологічної безпеки. У певні періоди часу та за відповідних умов одна з базових груп потреб може ставати провідною більшою мірою, ніж інші, визначаючи поведінку та діяльність. У зв'язку з цим вона може перебудовувати всю мотиваційну сферу. Потреба в безпеці стає домінантною в умовах турбулентних явищ, що руйнують звичні стереотипи поведінки

та сформований образ життя. Саме вона починає визначати мотивацію соціальної поведінки людини, перебудовуючи та змінюючи її, специфічним чином трансформуючи інші базові групи потреб, психічні особливості та характеристики особистості, тим самим змінюючи вектор розвитку на різних рівнях інформаційної безпеки. На особистісному рівні першочерговості набуває здатність до адаптації збитку психічному здоров'ю.

Проблеми інформаційної безпеки на сьогодні актуалізуються ще й тим, що значно зросла роль накопичення, обробки та поширення інформації, зокрема, в ухваленні стратегічних рішень, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Інформація стала одним із чинників, здатних привести до великомасштабних аварій, військових конфліктів і дезорганізації державного управління. Тому Україні необхідно приділяти своїй національній інформаційній безпеці особливу увагу, оскільки вона є основою життєво важливих інтересів особи, держави та суспільства. Для подолання турбулентності та досягнення керованості необхідна систематизація й алгоритмізація державних управлінських рішень.

Сучасне інформаційне середовище здатне впливати на психологічний стан соціуму через обсяг, достовірність, відповідність інформації потребам споживача та обставинам її отримання, наявність за сучасних інформаційних технологій специфічних елементів, що змінюють психічний стан людини і т.ін. Поряд із цим, і сама особистість стає джерелом інформаційно-психологічного ризику через незрілість та нездатність до фільтрації, переробки, відображення одержуваної певної інформації, особистісний конформізм, схильність до маніпулятивних дій іззовні, масове зараження ідеями, функціональні зміни психіки, психоемоційну нестабільність, інформаційний стрес, фрустрацію, тривожність і т.д.

Із метою збереження інформаційно-психологічної безпеки особистості необхідно забезпечити постійний контроль і аналіз усіх джерел підвищеного інформаційного ризику, завчасне про-

гнозування процесів їхнього прояву та оперативне відпрацювання адекватних контрзаходів, здатних відвернути чи хоча б мінімізувати небажані наслідки інформаційної турбулентності, яка є результатом синергетики властивостей інформаційного середовища та деструктивних факторів інформаційно-психологічної безпеки як по відношенню до держави, суспільства, так і до окремої особистості.

Нестабільне середовище продукує і високі ризики, і високі шанси для держави не втратити управлінські функції. Важливим завданням є інвентаризація досягнутого, розуміння нових реалій і вироблення відповідної державної політики. Успішне управління інформаційною безпекою в епоху турбулентності базується на чотирьох парадигмах: системна, синергетична, феноменологічна та когнітивна.

Базовими елементами механізму взаємодії між владою і суспільством у даній сфері є інституційна, нормативно-правова та практична складові. Від повноцінного використання всіх можливостей і ресурсів суспільства залежить ефективність функціонування всієї системи інформаційної безпеки держави.

Особлива роль відводиться засобам масової інформації, які поступово перетворюються на засоби масової комунікації. Вони поряд із органами державної влади можуть і повинні брати участь у забезпеченні інформаційної безпеки таким чином, щоб процес циркуляції інформації не переривався, інформація не спотворювалася, а права та інтереси її суб'єктів не обмежувалися.

Засоби масової інформації, звернені насамперед до масової аудиторії, природою своєю покликані забезпечити масово-інформаційну безпеку за рахунок доставки споживачам необхідних для прийняття рішень інформаційних ресурсів, захисту від маніпулятивного, рейкового контенту, дезінформації, що поширюються тими ж ЗМІ.

Загальнодержавна інформаційна політика повинна включати положення про необхідність активного ведення соціально-

го діалогу в ЗМІ з приводу проблем, до яких по-різному підходять різні соціальні сили.

Аналізуючи інформаційну безпеку, неможливо пропустити її розгляд у проекції на дитину. Дитяча психіка дуже вразлива по відношенню до інформаційних впливів унаслідок несформованості найважливіших психічних функцій і структур, що забезпечують адекватну переробку інформації і психологічний захист особистості. Спираючись на соціальні контексти розвитку, внутрішню позицію дитини та її ставлення до світу, інформаційна безпека дитини повинна враховувати два аспекти: захист від негативного впливу інформаційного середовища й розвиток умов, що забезпечують позитивну соціалізацію та індивідуалізацію дитини.

Дитина, будучи активним учасником суспільних відносин в інформаційній сфері, є найбільш незахищеним їхнім суб'єктом у силу вікового онтогенезу та підвищеної інформаційної вразливості, тому вона потребує особливого захисту з боку держави.

Проблема інформаційної безпеки дітей зумовлює вирішення комплексу питань, пов'язаних із упорядкуванням інформаційного простору України, поглибленням наукових досліджень щодо протидії шкідливому впливу ЗМІ, удосконаленням нормативно-правової бази по відношенню до суб'єктів інформаційної діяльності. Вирішення даної проблематики не може бути досягнуто без урахування гуманного чинника інформаційного середовища, оскільки заборонні функції держави сьогодні є малоефективними й нерідко стають об'єктом критики з боку інститутів громадянського суспільства. Необхідно також урахувати позитивний та негативний закордонний досвід щодо вирішення питань інформаційної безпеки дитини.

Інструментом практичного вирішення багатьох питань у сфері інформаційної безпеки дитини буде реалізація пріоритетних національних проєктів «Здорова дитина», «Якісна освіта», цільових програм, прийняття низки найважливіших законодавчих актів, спрямованих на підтримку прав дитини, серед яких

– закони: «Про інформаційну безпеку дітей», «Про ювенальну юстицію», «Про медіацію».

Важливим напрямком дослідження забезпечення інформаційної безпеки є медико-психологічний. Адже постійні стреси та емоційні навантаження можуть призводити до криз, тяжких душевних потрясінь. У такому стані людина змушена жити, пристосовуючись до довкілля.

Емоція тривоги – одне з найбільш частих переживань людей у критичних ситуаціях, яке за надзвичайних впливів може виконувати різні функції – як адаптивну, так і дезорганізуючу психічну діяльність.

Тривога, як психічний стан, і тривожність, як психічна властивість, знаходяться в конфронтації з базовими особистісними потребами: потребою в емоційному благополуччі, почутті впевненості, безпеки. Подібні явища властиві і інформаційно-психологічній турбулентності – новому поняттю, представленого в монографії. Задіяння турбулентного способу мислення, набутого як внутрішніми так і зовнішніми чинниками, є перспективним напрямом розвитку особистістю адаптаційних можливостей.

Необхідно розробляти нові напрямки медико-психологічної допомоги, направлені на зниження тривоги та підвищення адаптації до нових умов існування із застосуванням комплексних медико-психологічних заходів на державному рівні. Проблема надання спеціалізованої допомоги населенню має два важливих і принципових аспекти: психологічний і власне психіатричний, що обумовлюють необхідність комплексного підходу із залученням різноманітних фахівців суміжного профілю (психологів, психотерапевтів та ін.). Саме такий підхід здатний забезпечити не тільки своєчасну адекватну медико-психологічну допомогу, а й провести адресні психопрофілактичні та психокорекційні заходи, спрямовані на зниження тяжкості та вираженості психологічних, психічних, психосоматичних і соматичних наслідків екстремальних ситуацій, а також у найближчі та віддалені періоди після їх завершення. Тому важним державним

завданням є підготовка, перепідготовка відповідних висококваліфікованих професійних кадрів.

Теоретичним підґрунтям для нових підходів може стати запропонована авторська модель цілісного забезпечення інформаційно-психологічної безпеки, що передбачає як захист, так і відновлення психологічного благополуччя особистості, де базовими є такі процеси: реабілітація, абілітація, компенсація та адаптація. Усі вони, триваючи в часі, здійснюються на чотирьох рівнях своєї організації: біологічному, психологічному, соціальному, соціально-психологічному, і кожен із них має інформаційний супровід (паралельний інформаційний рівень).

Неможливо уявити ефективність заходів щодо інформаційної безпеки без її нормативно-правового регулювання. Сучасне становище останнього можна визначити як стан системи, що знаходиться в стадії формування, а тому неминуче несе риси перехідного етапу з певними проблемами правового забезпечення державного управління інформаційною безпекою. Запропонована концепція системи інформаційної безпеки органів державної влади, спрямована на підвищення ефективності їхньої діяльності, на захист інтересів держави, що, у свою чергу, включають інтереси особистості та суспільства. Будь-яка діяльність держави, у тому числі, у забезпеченні інформаційної безпеки, повинна ґрунтуватися у своїй вихідній точці на визнанні, дотриманні й захисті прав людини.

Для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства та забезпечення інформаційної безпеки.

Розроблена універсальна модель управління комплексною інформаційною безпекою держави на основі встановлених факторів турбулентності включає об'єкт контролю, суб'єкти контролю, ризики, виклики та стратегії. Індивідуальний

аналіз викликів на кожному з рівнів (державному, регіональному, місцевому, особистісному) дозволяє розробляти відповідне планування стратегій до кожного окремого випадку чи ситуації. Модель пояснює причини порушення стабільності будь-якої системи чи рівня інформаційної безпеки, оскільки вказує на різні варіанти можливої конфігурації: появу нових незвичних викликів і ризиків (зовнішніх і внутрішніх); провал колишніх суб'єктів контролю (інститутів, організацій, практик), надмірні витрати й незаплановані негативні наслідки їхньої діяльності; неадекватні стратегії відповіді на виклики; нерелевантність об'єктів контролю, виражених через цінності, принципи та правила, що змінилися.

На основі моделі є можливість формувати концептуальні положення державного управління у сфері інформаційної безпеки при реагуванні на турбулентні явища, які включають сукупність спеціальних практичних заходів, засобів, важелів, спрямованих на досягнення головної мети якнайшвидшої ліквідації деструктивних наслідків та відновлення нормальної життєдіяльності громадян, органів державного управління та місцевого самоврядування, підприємств тощо. Модель дозволяє вирішити головні завдання щодо забезпечення інформаційної безпеки, як складової національної безпеки держави.

Автор має надію, що монографія буде цікава широкому колу науковців і практиків державного управління, менеджерів, лікарів, психологів, журналістів, викладачів, студентів і стане дієвим джерелом інформації з проблематики державного управління задля збереження суспільного порядку, підтримання інформаційно-психологічного здоров'я населення в умовах турбулентних викликів.

Наукове видання

Олег Панченко

ІНФОРМАЦІЙНА БЕЗПЕКА В ЕПОХУ ТУРБУЛЕНТНОСТІ: ДЕРЖАВНО-УПРАВЛІНСЬКИЙ АСПЕКТ

(українською мовою)

МОНОГРАФІЯ

Редактор
Кабанцева А.В., к.психол.н.

Коректор
Хреннікова Л.А.

Відповідальний за випуск
Антонов В.Г.

Комп'ютерна верстка
Сікан Д.В.

Дизайн обкладинки
Черняк О.В.

Підписано до друку 25.06.2020. Формат 64 X 90 $/_{16}$.
Папір офсетний. Ум. друк. арк. 38,35.
Наклад 1000 прим. Зам № 280.

ТОВ «Комп'ютерно-видавничий інформаційний центр (КВІЦ)
04080, м. Київ, вул. Кирилівська 19–21, тел.: 482-50-68, 482-45-23
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи ДК № 461 від 23.05.2001 р.