НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ПАНЧЕНКО Олег Анатолійович

УДК 35:004.9

ДЕРЖАВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ЕПОХУ ТУРБУЛЕНТНОСТІ

25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора наук з державного управління

Харків, 2020

Дисертацією є рукопис.
Робота виконана в Міжрегіональній Академії управління персоналом.

Науковий консультант– доктор наук з державного управління, професор **ПАРХОМЕНКО-КУЦЕВІЛ Оксана Ігорівна**, ПрАТ "Вищий навчальний заклад "Міжрегіональна академія управління персоналом", професор кафедри публічного адміністрування.

Офіційні опоненти: доктор наук з державного управління, професор **КРЮКОВ ОЛЕКСІЙ ІГОРОВИЧ**, Національний університет цивільного захисту України, професор кафедри публічного адміністрування у сфері цивільного захисту навчально-науково-виробничого центру;

доктор наук з державного управління, доцент, Заслужений юрист України **НОНІК ВАЛЕРІЙ ВІКТОРОВИЧ,** Державний університет «Житомирська політехніка», проректор із науково-педагогічної роботи, юридичних та соціальних питань;

доктор наук з державного управління, професор **ГУРКОВСЬКИЙ ВОЛОДИМИР ІГОРОВИЧ**, Всеукраїнська громадська організація "Центр досліджень проблем публічного управління", перший заступник директора.

Захист відбудеться«29» жовтня 2020 року о 12.00 годині на засіданні спеціалізованої вченої ради Д 64.707.03 Національного університету цивільного захисту України за адресою: (61023, м. Харків, вул. Чернишевська, 94; тел. (057) 715-63-91).

Із дисертацією можна ознайомитись у бібліотеці Національного університету цивільного захисту України за адресою: 61024, м. Харків, вул. Чернишевська, 94.

Автореферат розісланий «28» вересня 2020 р.

Учений секретар
спеціалізованої вченої ради Н.С. Грабар

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Однією зі складових суспільного розвитку України є стабільність у системі державного управління інформаційною безпекою в епоху турбулентності. Участь громадськості в процесі державного управління є невід'ємним атрибутом будь-якої сучасної держави. Ефективність функціонування політичною системою держави у вирішенні складних соціально-політичних проблем сучасності безпосередньо пов'язане з роботою громадських об'єднань та окремих громадян. Найбільш яскраво ця залежність проявляється в умовах необхідності протидій загрозам національній безпеки держави. На даний час інформатизація набула статусу важливого об'єкта, стратегічного ресурсу як держави, так і будь-якої управлінської структури в системі політичного управління.

Розвиток нових інформаційних технологій обумовлює збільшення технологічного розриву між вимогами, які постійно ускладнюються до показників захищеності інформаційних ресурсів у суб'єктів державного управління України і можливостей інформаційних технологій та програмно-апаратних засобів, що використовуються при забезпеченні інформаційної безпеки. Варто зауважити, що поряд із цим, зростає потреба в науково обґрунтованих методах і технологічних рішеннях для поновлення і вдосконалення системи забезпечення інформаційної безпеки не тільки держави, а й суспільства й особистості зокрема. Саме тому на сучасному етапі розвитку України надзвичайно актуальним є вирішення проблеми державного управління у сфері інформаційної безпеки в часи турбулентності мислення суспільства. Істотною причиною цього, із одного боку, є недосконалі механізми державного управління цією сферою, а з іншого, – це зумовлюється недостатністю науково обґрунтованих методів і технологічних рішень для поновлення і вдосконалення системи забезпечення інформаційної безпеки України в епоху радикальних змін інформаційно-психологічного простору. Існуюча недосконалість діючої системи інформаційної безпеки призводить до колосальних збитків для держави, суспільства й особистості. Таким чином, актуальності набирає потреба в перезавантаженні діючої системи інформаційної безпеки у відповідності до сучасного суспільного запиту й турбулентних викликів. Для реалізації останнього нагальним виступає удосконалення таструктуризаціянормативно-правового, технічного, інформаційно-організаційного, медико-психологічного й превентивно-просвітницького функціоналу.

У процесі підготовки дисертаційного дослідження було використано фундаментальні праці науковців, у яких розкриваються різні аспекти державного управління інформаційною безпекою. Так, значний внесок у дослідження процесів забезпечення національної безпеки в контексті розвитку інформаційного суспільства зробили такі зарубіжні вчені, як: Е. Аронсон, Д. Белл, Х. Веріан, А. Зобнин, С. Кара-Мурза, М. Кастельс, К. Малапарте, Е. Тоффлер, Ю. Хабермас та ін.

Комплексному політологічному аналізу проблеми забезпечення інформаційної безпеки держави присвячені роботи О. Андрєєвої, І. Залєвської, В. Козубського, В. Конах, В. Петрова, та Ю. Романчука.

Безпосередньо питання державного управління у сфері інформаційної безпеки досліджували О. Власенко, В. Гурковський, Л. Євдоченко і З. Коваль.

Окремі аспекти обраної нами проблематики з позицій державного управління розглядали В. Абрамов, Р. Войтович, В. Горбулін, Н. Грицяк, В. Карлова, Д. Кучма, О. Литвиненко, В. Мандрагеля, Р. Марутян, Ю. Нестеряк, Н. Нижник, К. Павлюк, І. Пантелейчук, Т. Пахомова, О. Пухкал, А. Савков, С. Серьогін, Г. Ситник, В. Смолянюк, С. Соловйов, І. Сурай, О. Твердохліб, С. Телешун, М. Шевченко.

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек і загрозта здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм відповідно до чинного законодавства.

Вивчення законодавчих документів Верховної Ради України, а саме: Закону України «Про інформацію»,Закону України «Про національну безпеку України», Закону України «Про Національну програму інформатизації», Закону України «Про Концепцію Національної програми інформатизації», Закону України «Про друковані засоби масової інформації (пресу) в Україні», Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» та нормативно-правових актів Кабінету Міністрів України свідчать, що рівень державного управління національною системою інформаційної безпеки не відповідає новим соціально-економічним умовам і викликам сьогодення. Нагальною є потреба у формуванні якісно нової моделі управління інформаційною безпекою України, яка б відповідала вимогам сучасного соціального менеджменту, адаптованого до потреб галузі. Не менш важливим питанням, що потребує уваги наукової спільноти, є сприяння розвитку інформаційної культури відповідно до доктрини інформаційної безпеки України. Остання визначає повноваження та обов'язки органів влади, силових структур, додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту інтересів особистості, суспільства й держави в інформаційній сфері, національному інформаційному простору.

Науковий пошук комплексних заходів і методів вдосконалення системи інформаційної безпеки політичних структур, підвищення управлінського потенціалу, особливо органів виконавчої влади зумовлює високий ступень актуальності дисертаційного дослідження. Разом із тим, у роботі викладені на єдиних системних засадах основи національної безпеки держави, місце і роль інформаційної безпеки в системі національної безпеки держави в епоху суспільного хаосу, сутність інформаційних воєн як джерела інформаційних загроз національним інтересам держави. Як наслідок наявних наукових досліджень щодо розробки державно-управлінських аспектів забезпечення інформаційної безпеки, доводиться констатувати, що в системі державного управління до цього часу відсутні комплексні наукові дослідження, присвячені

теоретичним аспектам формування та функціонування системи державного управління забезпеченням інформаційної безпеки в умовах турбулентності.

Ураховуючи вищевикладене, нагальною проблемою, що потребує комплексного та системного вирішення в епоху турбулентності постає забезпечення інформаційної безпеки особистості, суспільства та держави, оскільки значно зросла роль накопичення, обробки й поширення інформації, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. У час суспільних змін, стрімкого розвитку інформаційних технологій, можливостей використання різних засобів впливу на людську свідомість, особливої актуальності набуває проблема психологічної безпеки особистості. Порушення інформаційно-психологічної безпеки у вигляді збитку психічному стану людини потребують своєчасного реагування у вигляді медико-психологічної допомоги, направленої на зміцнення стресостійкості та підвищення життєдіяльності. Дедалі гостріше постає проблема браку кваліфікованих управлінських кадрів у сфері інформаційної безпеки з високим рівнем професійних, ділових якостей, спроможних ухвалювати ефективні управлінські рішення. Наразі є необхідним подальше вдосконалення процесів і підходів до навчання й підвищення кваліфікації фахівців різних державних інституцій, діяльність яких пов’язана із захистом державних секретів і забезпеченням інформаційної безпеки. Питання управління національною інформаційною безпекою потребує першочергового вирішення з боку держави, оскільки воно є основою визначення найважливіших напрямів і принципів державної інформаційної політики країни.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано за темами науково-дослідних робіт державного закладу «Науково-практичний медичний реабілітаційно-діагностичний центр Міністерства охорони здоров’я України» «Розробка технології медико-психологічної реабілітації та соціальної абілітації дітей, які зазнали психологічного насилля» (ДР № 0120U101301), «Теоретико-методологічні основи державного регулювання та практики інформаційної безпеки в умовах турбулентності: політичні, юридичні, економічні, соціальні й психологічні проблеми» (ДР № 0120U100582), «Теоретико-методологічні засади державного регулювання медико-психологічної реабілітації та абілітації» (ДР № 0120U100628), де автор був керівником тем, у межах яких було проаналізовано міжнародний досвід та обґрунтовано теоретико-методологічні основи державного управління у сфері забезпечення національної інформаційної безпеки України в епоху турбулентності. У НДР «Розробка системи реабілітації медико-психологічного спрямування особам в умовах інформаційно-психологічної війни» (ДР № 0120U101304) автор був співвиконавцем.

Мета і завдання дослідження. Метою дисертаційної роботи є розробка та обґрунтування теоретико-методологічних засад державного управління у сфері забезпечення інформаційної безпеки суспільства та особистості в умовах турбулентності як складової національної безпеки України.

Відповідно до мети було поставлено такі *завдання*:

– дослідити теоретико-методологічні засади державного управління інформаційною безпекою в умовах турбулентності; визначити проблему дослідження;

– виокремити інформаційно-психологічні фактори турбулентно-політичного і соціально-економічного плану «інформаційного хаосу» та дати авторське визначення поняття «епоха турбулентності»;

– дослідити сучасний стан нормативно-правового регулювання інформаційної безпеки;

– проаналізувати зв'язок між турбулентністю й метаморфозами суспільства, визначити його вплив на інформаційну безпеку як держави та суспільства, так і окремої особистості;

– обґрунтувати аксіологічне бачення інформаційно-психологічної безпеки та розробити модель щодо її забезпечення;

– обґрунтувати комплексний підхід до визначення стратегії розвитку системи інформаційної безпеки в умовах глобалізації;

– запропонувати варіант вирішення проблем державного управління у сфері забезпечення інформаційної безпеки в умовах турбулентності;

– аргументувати необхідність запровадження нової сучасної концепції розвитку державного управління у сфері забезпечення інформаційної безпеки;

– систематизувати та визначити сучасну конфігурацію принципів державного управління у сфері забезпечення інформаційної безпеки громадян;

– розробити універсальну модель підтримки рівноваги стану динамічної системи забезпечення інформаційної безпеки;

– запропонувати концептуальні засади державного управління у сфері інформаційної безпеки при реагуванні на турбулентні явища, що загрожують національній безпеці.

Об'єктом дослідження є система забезпечення інформаційної безпеки держави.

Предметом дослідження є державне управління забезпеченням інформаційної безпеки України в умовах турбулентності.

Методи дослідження. В основу методологічного дослідження роботи покладено систему загальнонаукових та спеціальних, емпіричних і теоретичних методів дослідження, зокрема:

теоретико-методологічний аналіз – для визначення актуального стану наукових розробок та нормативно-правової бази щодо державного регулювання інформаційною безпекою;

інституційний метод – представлений комплексом усе загальних, загальнонаукових та спеціальних методів наукового пізнання, який дозволив провести аналіз діяльності органів державної влади, що складають систему забезпечення інформаційної безпеки держави;

порівняльно-ретроспективний аналіз й абстрагування – для встановлення змісту та етапності розвитку державного управління, причинно-наслідкових зв'язків застосування безпеки державного управління;

психодіагностичні методи (бесіда, спостереження, анкетування, тестування) – для встановлення інформаційно-психологічного впливу на свідомість суспільства та актуального психоемоційного стану останнього;

аналіз емпіричної та статистичної інформації – для визначення тенденцій щодо змін державно-суспільних відносин та актуальних напрямів підвищення дієвості державного управління;

метод індукції полягав в узагальнені та систематизації емпіричного матеріалу для проведення комплексного аналізу забезпечення інформаційної безпеки, визначення засобів та інструментів державного управління в досліджуваній сфері, об'єднання цілей і сфер управління;

метод дедукції – для з'ясування цілей управлінських впливів державного управління;

системний метод (системний аналіз та синтез) – дозволив ґрунтовно підійти до розгляду структурних складових системи забезпечення інформаційної безпеки;

аксіологічний – вивчення потреб, що відповідають особистим запитам і нормам суспільства у стані соціально-економічної і психологічної нестабільностей із метою формування нової онтологічної картини управління у сфері забезпечення національної інформаційної безпеки в епоху турбулентності;

Застосовані в сукупності методи дозволили виявити пріоритетні управлінські рішення та розробити рекомендації щодо оптимізації діяльності забезпечення інформаційної безпеки у сфері державного управління.

Наукова новизна одержаних результатів полягає в новому систематизованому комплексному дослідженні інформаційної безпеки особистості, суспільства, державних інституцій та в розробці теоретичних і практичних шляхів удосконалення стратегії державного управління інформаційною безпекою в умовах турбулентних викликів.

Найсуттєвіші результати дисертаційного дослідження, які містять наукову новизну, полягають у тому, що:

уперше:

– розроблено та науково обґрунтовано концептуальні засади щодо вдосконалення системи державного управління інформаційної безпеки як основи її функціонування в умовах турбулентності, основними напрямами формування яких визначено: удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки; концентрацію діяльності органів державної влади й ресурсів держави на пріоритетних завданнях розвитку інформаційного суспільства та забезпечення інформаційної безпеки; 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; цілеспрямоване впровадження позитивних

результатів і урахування недоліків зарубіжного досвіду щодо організації та проведення інформаційних операцій, форм, методів, засобів запобігання кібератакам, а також моделювання та прогнозування інформаційних нападів;

– сформовано методологічне підґрунтя щодо забезпечення інформаційної безпеки держави як основи її функціонування, яке включає необхідність нормативно-правового регулювання щодо протидії використання інформаційних технологій, що загрожують інтересам держави, створення економічних передумов для розвитку національних інформаційних ресурсів та інфраструктури, впровадження новітніх технологій в інформаційну сферу; виявлені та систематизовані організаційні підходи формування управлінських рішень у системі інформаційної безпеки України, а саме: системний, синергетичний, феноменологічний та когнітивний підходи;

– розроблено модель формування системи державного управління у сфері інформаційної безпеки дитини задля покращення становища дітей та удосконалення їх захисту, що вміщує п’ять складових: реінтеграція мікросоціуму, «Comeback» прав і обов'язків, усвідомлення відповідальності, комплексна реабілітація суб'єктів конфлікту, ресоціалізація;

– запропоновано комплексний підхід до визначення стратегії розвитку системи інформаційної безпеки в умовах глобалізації, який поєднує функціонування систем захисту інформації, високий рівень технічного й нормативно-правового забезпечення та конкурентоспроможну професійну компетенцію державних службовців;

удосконалено:

– пріоритетні управлінські механізми та деструктивні фактори інформаційного середовища в стані турбулентності, що полягають у захисті 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;

– організаційно-методичне забезпечення професійної кадрової складової інструментарієм та запобіжниками розладів психічної сфери під час застосування інформаційних атак та інших інформаційно-психологічних впливів, та підходи до оцінювання особливостей організаційно-правових засад управлінської діяльності під час вирішення проблем, які виникають у зв’язку з інституційними змінами в галузі інформаційної безпеки України.

– модель підтримки рівноваги стану динамічної системи забезпечення інформаційної безпеки, яка містить такі основні складові як суб’єкти контролю, ризики, виклики і стратегії, що дозволяє оцінити ризики інформаційних викликів епохи турбулентності та сформувати дієві напрямки державного політики підтримки рівноваги цієї системи.

набули подальшого розвитку:

– напрями забезпечення національної безпеки при об'єктивізації небезпеки збитку у вигляді насильства як на особистісному рівні, так і на

державному, що враховує наступні конструкти: превенція; збереження, захищеність, нарощування національних цінностей; усунення збитку, завданого насильством; постпревенційні організаційно-правові заходи для мінімізації можливого збитку, завданого насильством;

– понятійно-категорійний апарат у контексті наукової галузі державного управління, зокрема, уведення до наукового обігу таких понять: «епоха турбулентності», «інформаційно-психологічна турбулентність особистості», «турбулентне мислення», «інформаційно-психологічна абілітація»;

– теоретичне обґрунтування ролі органів державної влади в реалізації безпекової політики в управлінській сфері інформаційної діяльності в рамках державного управління та в покращенні організації системи якісної підготовки спеціалістів в області інформаційної безпеки, розробки організаційних та технічних заходів із захисту інформації;

Практичне значення одержаних даних полягає в тому, що розроблені теоретичні положення доведені до рівня конкретних практичних пропозицій (прогнозування і своєчасне виявлення загроз безпеки інформаційних ресурсів, причин і факторів, що сприяють нанесенню шкоди, порушення нормального функціонування й розвитку; створення умов функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і нанесення різних видів шкоди; забезпечення механізму й умов оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки; створення умов для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб), які можна використовувати в діяльності Офісу Президента України, Кабінету Міністрів України, органів місцевого самоврядування, громадських та політичних організацій України. Науково-методичні розробки (концептуальні засади розвитку державного управління у сфері забезпечення інформаційної безпеки при реагуванні на турбулентні явища, модель забезпечення національної безпеки в разі об'єктивізації небезпеки збитку у вигляді насильства, модель підтримки рівноваги стану динамічної системи забезпечення інформаційної безпеки, модель формування системи державного управління у сфері інформаційної безпеки дитини) дисертаційної роботи можуть бути використані у законотворчій діяльності, зокрема в розробці Національної стратегії та концепції інформаційної безпеки, у науково-дослідницькій сфері при розробці фундаментальних праць у галузі державного управління та місцевого самоврядування, інформаційної політики, теорії управління, що стосується розвитку регулювання сфери інформаційної безпеки України.

Результати дисертаційного дослідження знайшли своє конкретне практичне застосування в роботі Головного управління Держпродспоживслужби в м. Києві (довідка про впровадження №12.0/15392 від 08.05.2020), Головного управлінні Держпродспоживслужби в Житомирській області (довідка про

впровадження № 13-00/7-116від 27.05.2020), виконавчого комітету Дружківської міської ради (довідка про впровадження № 2326/1/130.145/1-20 від 19.05.2020).

Не менш показовим є також використання запропонованих у дисертаційному дослідженні теоретичних підходів, висновків та рекомендацій щодо засад державного управління у сфері забезпечення інформаційної безпеки суспільства та особистості в умовах турбулентності у викладацькій і навчально-методичній діяльності Національного університету «Одеська юридична академія» (акт впровадження від 19.05.2020).

Окремі висновки та положення, обґрунтовані в дисертації, використані в діяльності громадської організації «Всеукраїнська асамблея докторів наук із державного управління» (довідка про впровадження № 1722/2/2020 від 15.04.2020).

Результати дослідження та розроблені на їх основі висновки створюють підґрунтя для подальшого виокремлення нового теоретико-методологічного та практичного підходу до модернізації державної політики у сфері забезпечення інформаційної безпеки України. Запропоновані в досліджені наукові положення, висновки й рекомендації можуть бути використані в роботі центральними та місцевими органами влади, органами місцевого самоврядування в процесі розробки цільових програм із підвищення рівня інформаційного захисту населення.

Особистий внесок здобувача. Дисертаційне дослідження є виконаною особисто здобувачем науковою працею. Сформульовані в дисертації наукові результати, висновки, рекомендації і пропозиції належать авторові. Конкретний внесок здобувача в спільних публікаціях вказано в переліку основних публікацій.

Апробація результатів дисертації. Основні положення та результати дослідження доповідались і обговорювались на міжнародних та всеукраїнських науково-практичних конференціях, зокрема: на ІІІ міжнародній науково-практичній конференції «Проблеми підвищення рівня безпеки, комфорту та культури дорожнього руху» (Харків, 2013), на ІІ міжнародній науково-практичній конференції «Актуальні питання соціальної та практичної психології в координатах сучасних парадигм» (Луганськ 2014), на V міжнародній науково-практичній конференції «Когнітивні процеси та творчість» (Одеса, 2014), на IV міжнародній науково-практичній конференції «Соціалізація і ресоціалізація особистості в умовах сучасного суспільства» (Київ, 2014), на науково-практичній конференції з міжнародною участю «Медична і психологічна реабілітація й абілітація» (Костянтинівка, 2014), на всеукраїнській науково-практичній конференції «Діяльністно-поведінкові фактори життєздатності людини» (Харків, 2014), на міжнародній науковій конференції «Педагогіка і психологія в епоху зростаючого потоку інформації – 2015» (Будапешт, Угорщина, 2015), на міжнародній конференції «Шляхи реформування національної системи безпеки дорожнього руху. Безпечні дороги» (Київ, 2015), на Європейському конгресі з психології 2015 (Мілан Італія, 2015), на ІІІ міжнародному конгресі «Медицина транспорту – 2015» (Одеса, 2015), ІСТМ

2015 International Conference on ICT Management for Global Competitiveness and Economic Growth in Emerging Economies (Вроцлав, Польща, 2015), на міжнародній науково-практичній конференції «Психологічна допомога особистості в кризових соціокультурних умовах» (Київ, 2015), на міжнародній науково-практичній конференції «Безпека дорожнього руху: правові та організаційні аспекти» (Київ, 2015), на міжнародній науково-практичній конференції «Кримінально-виконавча політика України та Європейського Союзу: розвиток та інтеграція» (Київ, 2015), на всеукраїнському з міжнародною участю віртуальному Інтернет-семінарі «Інноваційні процеси в медицині та медичній інформатиці» (2015), на круглому столі «Досвід та перспективи психологічної реабілітації населення України» (Київ, 2016), на ІІ міжнародній науково-практичній конференції «Соціальні, психологічні та політичні проблеми транскордонної безпеки» (Одеса, 2016), на міжнародній науково-практичній конференції «Досвід України та країн Європейського союзу у вирішенні актуальних проблем психології в сучасних соціально-політичних умовах» (Київ, 2015), на науково-практичній конференції «Медико-психологічна допомога при постстресових станах: діагностика, лікування, реабілітація» (Костянтинівка, 2016), на науково-практичній конференції «Актуальні аспекти безпеки дорожнього руху в Україні. Стратегія і план дій. Безпека транспортних засобів та їх експлуатація» (Київ, 2017), на І міжнародному конгресі з питань реформування системи управління безпеки дорожнього руху (Київ, 2017), на лекції для співробітників поліції «Інформаційна безпека в умовах громадянського конфлікту» (Костянтинівка, 2017), на лекції для співробітників Костянтинівської райдержадміністрації «Інформаційна безпека особистості в умовах громадянського протистояння» (Костянтинівка, 2017), на лекції для співробітників Управління освіти Костянтинівської міської ради «Інформаційна безпека особистості в умовах громадянського протистояння» (Костянтинівка, 2017), на науково-практичній конференції з міжнародною участю «Медико-психологічні виклики сучасності» (Костянтинівка, 2017), на IV міжнародній науково-практичній конференції «Сучасний стан розвитку екстремальної та кризової психології» (Харків, 2017), на міжвузівській науково-практичній конференції «Економічні та гуманітарні проблеми розвитку сучасної України» (Краматорськ, 2017), на науково-практичній конференції «Сучасні проблеми психіатрії, психотерапії, наркології і неврології в умовах АТО в східному регіоні України» (Краматорськ 2017), на всеукраїнській науково-практичній конференції «Психосоціальна підтримка осіб із травмою війни: міжнародний досвід та українські реалії» (Маріуполь, 2018), на XI щорічній науково-практичній конференції «Становлення та розвиток особистості в умовах інформаційної війни» (Київ, 2018), на міжнародній науково-практичній конференції «Нове та традиційне в дослідженнях сучасних представників психологічних та педагогічних наук» (Львів, 2018), на інтернаціональній психологічній конференції «INPACT» (Порту, Португалія, 2018), на міжнародній науково-практичній конференції «Інтеграційний розвиток особистості та суспільства: психологічні і соціологічні виміри» (Одеса, 2018), на науково-

практичній конференції з міжнародною участю «Реалізація тривоги у психічні та соматичні розлади в населення в зоні проведення антитерористичної операції» (Костянтинівка, 2018), на міжнародній науково-практичній конференції «Інформаційні системи та технології в медицині» ISM–2018 (Харків, 2018), на XIV міжнародній науково-практичній конференції «Соціалізація особистості в умовах системних змін: теоретичні і прикладні проблеми» (Київ, 2019), на науково-практичній конференції «Актуальні проблеми модернізації недержавного сектору освіти в Україні в контексті світових тенденцій і національної практики». (Київ, 2019), на міжнародному конгресі з безпеки на транспорті (Київ, 2019), на науково-практичній конференції «Надання психіатричної та психологічної допомоги хворим на психічні розлади: сучасні виклики та реалії» (Краматорськ, 2019), на міжнародній науково-практичній конференції «Інформаційні системи та технології в медицині» ISM-2019 (Харків, 2019), на XIX міжнародній науково-практичній конференції «Реабілітаційна медицина та розвиток санаторно-курортних закладів» (Київ, 2019), на III міжнародній науковій конференції «Модернізація освітньої системи: світові тенденції та національні особливості» (Каунас, Литва, 2020), на V міжнародній науково-практичній конференції «Розвиток української держави в умовах активізації євроінтеграційних процесів» (Київ, 2020), на II міжнародній науковій конференції «ScienceandGlobalStudies» (Братислава, Словаччина, 2020), на II міжнародній науково-практичній конференції «Інтеграційний розвиток особистості і суспільства: психологічний та соціологічний вимір» (Одеса, 2020), на науково-практичній конференції «Публічне управління в цифровому суспільстві» (Дніпро, 2020).

Публікації. Основні ідеї, положення та результати дисертаційного дослідження опубліковано в67 наукових працях, зокрема в 10 монографіях (трьох індивідуальних та сімох – у співавторстві), у 22 статтях у наукових фахових виданнях із державного управління, у 5 статтях у закордонних наукових виданнях, у 8 статтях в інших наукових журналах, збірниках наукових праць, у 22 тезах доповідей та матеріалів наукових конференцій, семінарів та круглих столів.

Структура та обсяг дисертації. Дисертаційна робота загальним обсягом 456 сторінок складається зі вступу, п’яти розділів (що включають 55 рисунків, 8 таблиць) та висновків, а також додатків на 28 сторінках і списку використаних джерел із 327 найменування на 35 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертації, формулюються проблема, мета, завдання і методи дослідження, визначається наукова новизна й практичне значення одержаних результатів, їхня реалізація, особистий внесок здобувача, дані про публікації, ступінь апробації результатів дисертаційного дослідження.

У першому розділі – «Теоретико-методологічні засади державного управління у забезпеченні інформаційної безпеки в епоху турбулентності»– визначено теоретико-методологічні засади забезпечення інформаційної безпеки в епоху турбулентності, здійснено аналіз і систематизацію понятійно-категоріального апарату «інформаційна безпека» в системі національної безпеки, сформульовано визначення інформаційної безпеки в контексті національної безпеки, сформульовано визначення епохи турбулентності, визначено найбільш суттєві групи інформаційно-технічних небезпек, проаналізовано законодавче забезпечення та нормативно-правове регулювання формування й реалізація державної інформаційної політики України в сучасних умовах суспільного розвитку.

Акцентовано увагу на тому, що 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. При такому підході сформульовано визначення інформаційної безпеки як стану інформаційного середовища, що 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 дисертант вважає 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». Доведено, що інформаційна безпека займає ключове місце в системі національної безпеки держави. Виділено 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.

Визначено найбільш суттєві групи інформаційно-технічних небезпек. Перша група пов'язана з бурхливим розвитком нового класу зброї – інформаційної, що здатна ефективно впливати на психіку, свідомість людей і на інформаційно-технічну інфраструктуру суспільства. Друга група інформаційно-технічних небезпек для особи, суспільства й держави – це новий клас соціальних злочинів, що ґрунтуються на використанні сучасних інформаційних технологій. Третя група інформаційних небезпек – використання нових інформаційних технологій у політичних цілях.

Акцентовано увагу на складностях у сфері державного регулювання інформаційною безпекою, а саме: 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, окреслено основні проблеми забезпечення інформаційної безпеки в епоху турбулентності, серед яких є 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 органів державної влади до застосування ефективних технологій управління й організації взаємодії з громадянами й господарюючими суб'єктами; недостатній рівень підготовки кадрів в області створення і використання інформаційних і комунікаційних технологій. Вирішення проблеми забезпечення інформаційної безпеки суспільства та особистості повинно носити комплексний системний характер і здійснюватися на різних рівнях: нормативному, інституційному, що має на увазі узгоджену діяльність різних соціальних інститутів, пов'язаних із вихованням і соціалізацією, та особистісному, що пов'язаний, перш за все, із самовихованням, самоосвітою, формуванням високого рівня інформаційної культури особистості як частини загальної культури людини.

Сформульовано визначення епохи турбулентності, як історичний період, коли частішають і загострюються 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. Окреслені основні риси та ознаки епохи турбулентності. Визначено, що для подолання турбулентності й досягнення керованості необхідна систематизація та алгоритмічне використання відповідних суспільно-державних механізмів. Доведено, що з позиції системного підходу, система забезпечення інформаційної безпеки являє собою відкриту систему зі специфічними структурними елементами, яка має власні внутрішні зв’язки і зв’язки з навколишнім середовищем, а також функціонує та розвивається під впливом численних факторів.

Наголошено на тому, що проблеми інформаційної безпеки на сьогодні актуалізуються значним зростанням ролі накопичення, обробки й 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. І чим вище рівень інтелектуалізації й інформатизації суспільства, тим надійніше його інформаційна безпека. Тому Україні необхідно надавати своїй національній інформаційній безпеці особливої уваги, оскільки вона є основою визначення найважливіших напрямів і принципів державної політики країни, життєво важливих інтересів

особи, держави та суспільства.

Акцентуація на інформаційно-психологічному аспекті безпеки особистості, суспільства й 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 умовах турбулентної сучасності. За останній час 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. Тому, ураховуючи темп сучасного життя й техногенного розвитку, життєві потреби сучасної людини, дисертантом представлена модернізована піраміда людських потреб, що вміщує 7 рівнів (рис. 1.).

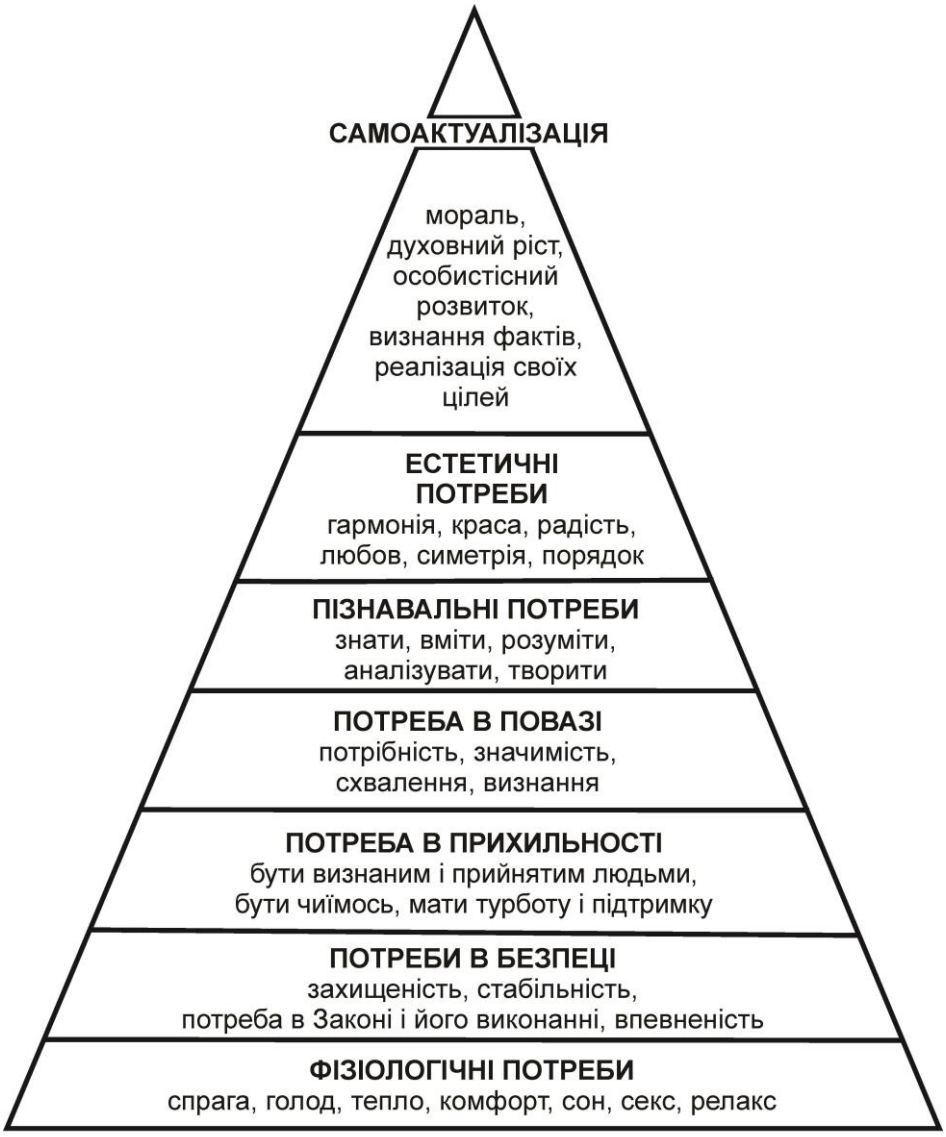

Рис. 1. Модернізована О. Панченком піраміда людських потреб А. Маслоу

За результатами дослідження зазначено, що 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 й державу. Основними принципами інформаційної безпеки є забезпечення конфіденційності, доступності, цілісності й автентичності інформаційних ресурсів та інфраструктури, що її підтримує.

У контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки визначено 8 факторів (об'єктивні та суб'єктивні) (рис. 2.). 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.

Проаналізовано законодавче забезпечення та нормативно-правове регулювання формування й реалізації державної інформаційної політики України в сучасних умовах суспільного розвитку. Показано, що інформаційну безпеку України становлять три структурні елементи: інформаційна безпека у сфері прав і свобод людини та громадянина, інформаційно-психологічна безпека, інформаційно-технічна безпека.

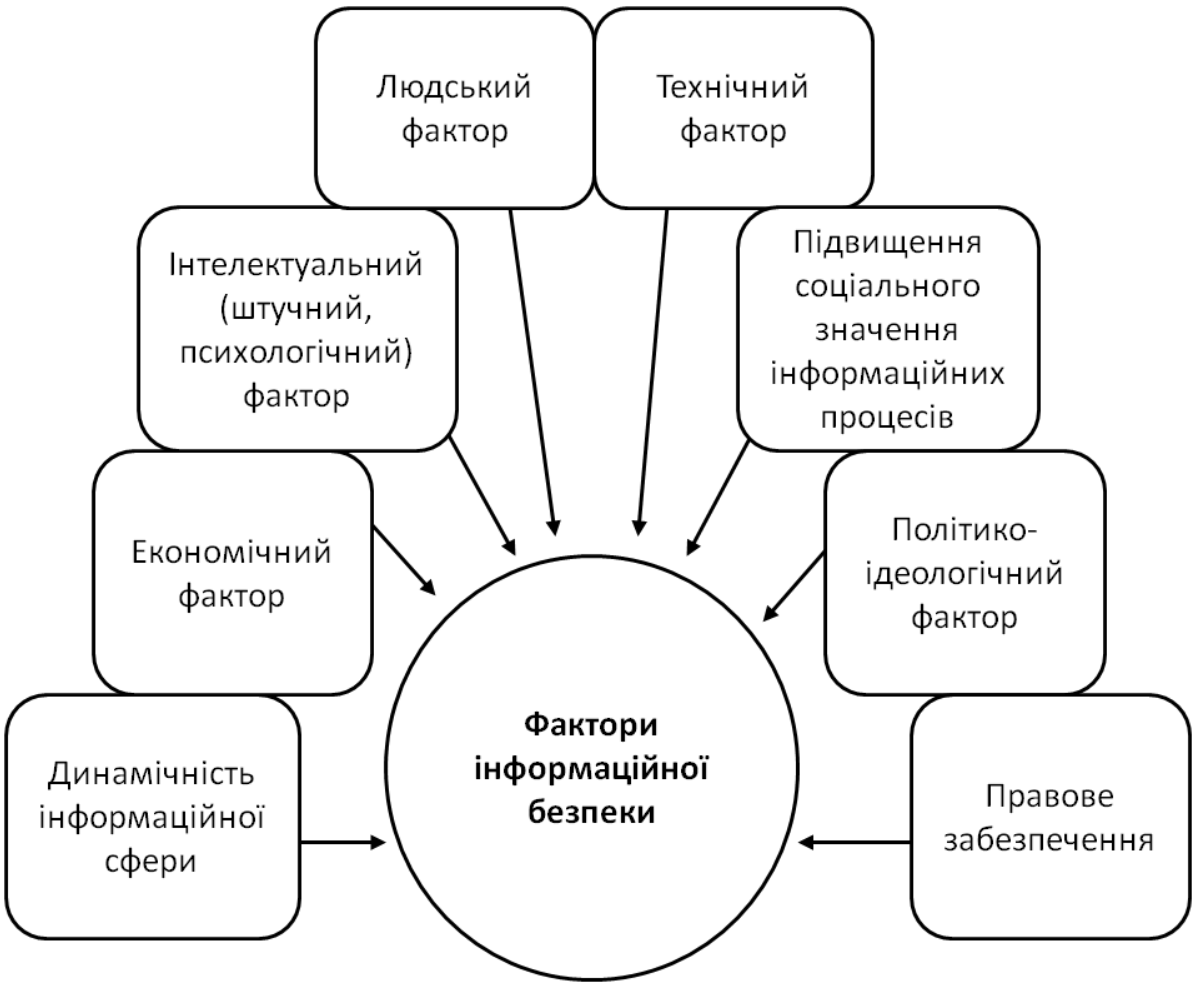

Рис. 2. Фактори інформаційної безпеки

Зазначено, що 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.

Наголошено на тому, що найважливіше завдання в справі забезпечення інформаційної безпеки держави – здійснення комплексного врахування національних інтересів особистості, суспільства й держави в даній сфері (рис. 3).

Виявлено основні проблемні питання, пов'язані з нормотворчістю в цій предметній сфері, оскільки аналіз взаємовпливу держави, суспільства й інформації перетворюється на одну з найважливіших теоретико-методологічних і практико-орієнтованих проблем сьогодення, а також узагальнено підходи до вдосконалення нормативно-правової бази щодо державного регулювання інформаційної політики в Україні

У другому розділі – «Стан державного управління інформаційною безпекою в умовах суспільно-інформаційної турбулентності» – проаналізовано зв'язок між турбулентністю й метаморфозами суспільства, результати яких свідчать про наявність причинно-наслідкового зв'язку. 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. Хаотичні нелінійні процеси, що мають вирішальний вплив на життя сучасної людини, неможливо редукувати за універсальними правилами. Тут потрібне більш «тонке» налаштування.

Визначено, що інформаційна турбулентність є наслідком синергетики властивостей інформаційного середовища та деструктивним фактором інформаційно-психологічної безпеки як у відношенні до держави і суспільства, так і окремої особистості. Інформаційне насильство поряд із економічним та політичним є системоутворюючим фактором соціального насильства. 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. Доведено, що 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. Характер інформаційних потреб суб'єктів національної безпеки визначає зміст інформаційного забезпечення національної Політика

інформаційної безпеки повинна бути орієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки всіх суб'єктів сфери інформатизації, бо інформаційне забезпечення національної безпеки являє собою процес задоволення інформаційних потреб суб'єктів національної безпеки.

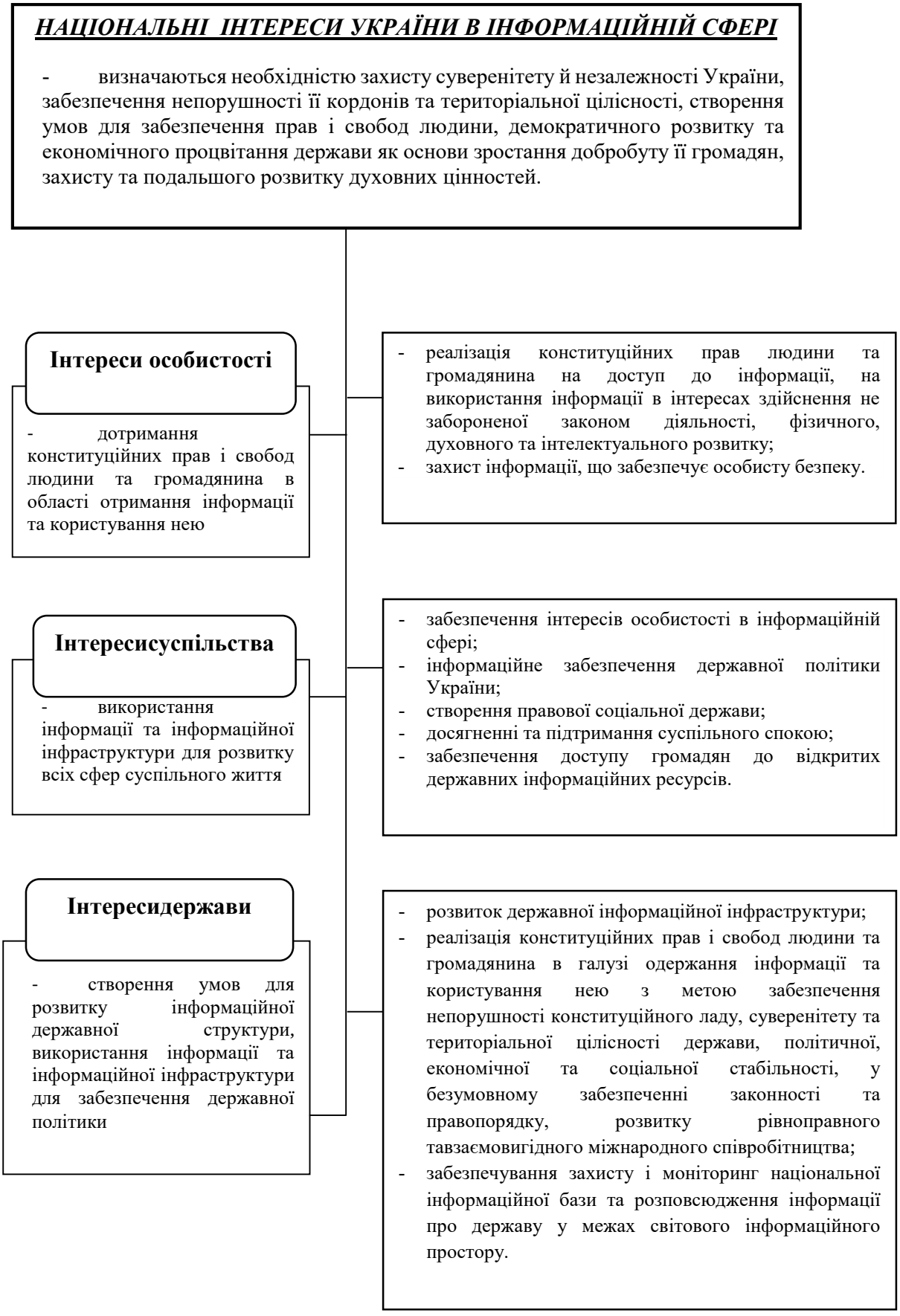

Рис. 3. Національні інтереси України в інформаційній сфері

Зазначено, що 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.

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. 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. Наступною важливою рисою ІС є складність і неоднозначність. 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 однозначно визначити характер впливу ІС – чи є сприйнята інформація корисною, нейтральною або шкідливою.

До факторів інформаційного середовища, здатних впливати на психологічну безпеку соціуму, слід віднести якісну та кількісну характеристику інформації (обсяг, справжність, кількість та інше), відповідність характеристик інформації параметрам реципієнтів та установкам навколишнього середовища, наявність за сучасних інформаційних технологій специфічних елементів, що змінюють психічний стан людини, наявність в інформаційних потоках удосконалених фізичних носіїв інформації, які впливають безпосередньо на фізіологічні носії. Однак, інформаційне середовище не єдине джерело ризиків для суспільства, а й сама особистість може бути джерелом формування факторів інформаційно-психологічного ризику, серед яких можна виділити незрілість і нездатність до фільтрації одержуваної інформації, особистісний конформізм, схильність до маніпулятивних дій іззовні, масове зараження ідеями, функціональні зміни психіки, психоемоційний стрес, фрустрацію, тривожність. Із метою збереження інформаційно-психологічної безпеки людини треба забезпечити постійний контроль і аналіз усіх джерел підвищеного інформаційного ризику, завчасне прогнозування процесів їхнього прояву та оперативне відпрацювання адекватних контрзаходів для відвернення чи мінімізації небажаних наслідків.

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.

Інформаційне насильство поряд з економічним та політичним є системо утворюючим фактором соціального насильства. На основі аксіологічного підходу пропонується авторська модель забезпечення національної безпеки в разі об'єктивізації небезпеки збитку у вигляді насильства (рис. 4), що враховує наступні конструкти: превенція; збереження, захищеність, нарощування національних цінностей; усунення збитку, завданого насильством; постпревенційні організаційно-правові заходи для мінімізації можливого збитку, завданого насильством.

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.

Рис. 4. Модель забезпечення національної безпеки при об'єктивізації небезпеки збитку у вигляді насильства

За умов 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 та делегувати більш широкі повноваження місцевому самоуправлінню, суспільним та громадським інститутам, які є більш динамічними в розрахунку-вимірі ризиків і управлінні ними.

У третьому розділі –«Засади формування системи державного управління у сфері інформаційної безпеки дитини» – визначені інформаційні ризики безпеки дитини в турбулентному інформаційному середовищі, наведено статистичні дані використання дітьми і підлітками інформаційних технологій, соціальних мереж і загального Інтернет-простору. Систематизовано міжнародні нормативно-правові документи щодо інформаційної безпеки дитини. Сформульовані напрямки захисту інформаційної безпеки дитини, розроблено модель формування системи державного управління у сфері інформаційної безпеки дитини, запропоновано інструментарій практичного вирішення широкого кола проблем інформаційної безпеки.

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.

Результати власних досліджень підтверджують, що дитина, будучи активним учасником суспільних відносин в інформаційній сфері, є найбільш незахищеним їх суб’єктом в силу вікового онтогенезу та підвищеної інформаційної вразливості, тому вона потребує особливого захисту з боку держави. Для забезпечення ІБ дитини державі необхідно застосувати комплексну систему захисту у трьох основних напрямках (рис. 5).

Рис. 5.Напрямки системи захисту інформаційної безпеки

Перший напрямок полягає у захисті інформації, інформаційних ресурсів та забезпечення надійного функціонування інформаційно-комунікаційних систем, у

тому числі систем критичної інфраструктури.

Другий – 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;

Третій напрямок реалізується у вихованні в особи навичок та умінь із підвищення її інформаційної безпеки.

Ураховуючи всі інформаційні, соціально-психологічні, нормативно-правові ризики, яких може зазнати дитина, окремим питанням у державному управлінні інформаційною безпекою дітей виступає розбудова ювенальної юстиції, так як на останнє покладається правове забезпечення повноцінного багатогранного сталого розвитку дитини й загальної національної безпеки взагалі.

Задля досягнення окресленої мети доцільним є застосування системного підходу. Для реалізації останнього і, ураховуючи результати власних теоретично-прикладних досліджень, розроблено авторську модель формування системи державного управління у сфері інформаційної безпеки дитини. Конструктив моделі вміщує п’ять складових, що логічно взаємодіють між собою(рис. 6).

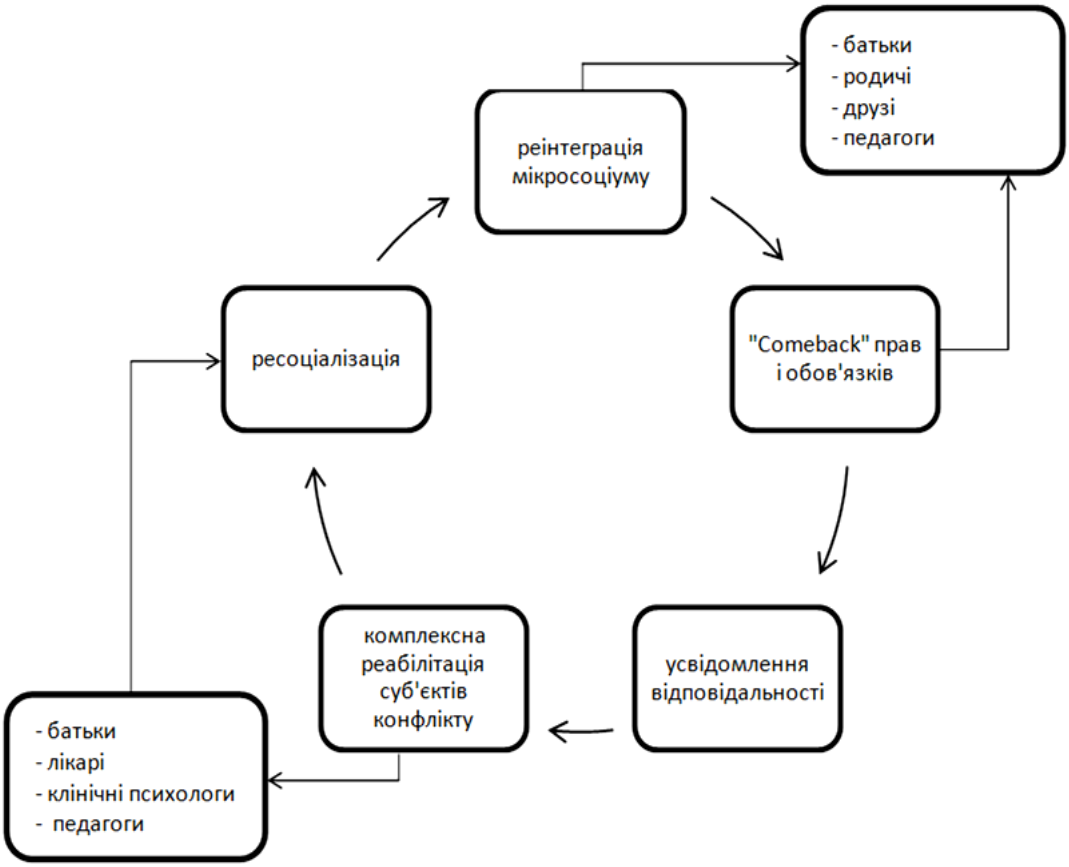

Рис. 6. Модель формування системи державного управління у сфері інформаційної безпеки дитини

Для кожної з цих складових характерні свої суб’єкти, власні функції і завдання, досягнення яких складають умови для наступної складової і подальшої роботи в межах всієї моделі.

Перша складова моделі – «Реінтеграція мікросоціуму». Ураховуючи функціонал ювенальної юстиції, вектор діяльності її представників, спрямований на взаємний процес суб’єктів соціально-правових відносин, під час якого змінюються всі зазначені. При цьому суб’єктами соціально-правових відносин виступають правопорушник, жертва, їхні батьки, родичі, друзі, педагоги. Підліток – як будь-яка інша людина, істота соціальна, живе, функціонує і розвивається у навколишньому світі, вступаючи в контакти з іншими людьми. І сім’я є тим першим найближчим середовищем, що безпосередньо впливає на формування особистості підлітка. Тому для того, щоб змінити поведінку і поведінкові реакції останнього, потрібно починати з сім’ї. Налагодження взаємовідносин і формування позитивного психологічного клімату, як у сім’ї правопорушника, так і в сім’ї жертви.

Друга – «"Comeback" прав і обов'язків». «Comeback», у перекладі з англійської, означає «повертатися», тобто повертатися до того, що вже було чи мав. Таким чином, дана складова включає повернення або точніше відновлення прав і свобод, обов’язків суб’єктів соціально-правових відносин. Особливо важливим у цьому виступає інформування про права і свободи жертви, обов’язки правопорушника і його батьків щодо відповідальності і виховання останнього. Особа, яка відчула порушення своїх громадянських прав і свободи, зазнала шкоди фізичного, психологічного, психічного, матеріального та будь-якого іншого характеру, цілком має можливість претендувати на ліквідацію втрат із подальшим відновленням отриманих збитків, зокрема, пов’язаних зі станом свого здоров’я та самопочуття.

Третя складова «Усвідомлення відповідальності» включає прийняття правопорушником на себе відповідальності за скоєну ним шкоду й усвідомлення потреби в усуненні цієї шкоди. На цьому етапі відбувається трансформація актуальних життєвих потреб, підвищується вмотивованість до ведення здорового способу життя, загальноприйнятої поведінки. Саме під час проходження цих кроків підліток набуває досвіду відповідального дорослого.

Четверта складова «Комплексна реабілітація суб'єктів конфлікту». Беззаперечно, будь-яке правопорушення чи злочин супроводжуються наявністю негативних особистісних проявів, рис характеру, поведінкових реакцій, шкідливих звичок, хімічної чи нехімічної залежностей. Тому комплексна реабілітація є ключовим фактором у відновленні особистості й успішної її соціалізації. Поряд із цим, реабілітації потребують власне жертви, які зазнали фізичного, психологічного та інших видів насильства. Отже, реабілітації підлягають як жертви, так і правопорушники, а також батьки перших і других. Процес реабілітації включає такі види впливу, як-от: медичний, психологічний, соціальний, педагогічний. Початком виступає комплексна діагностика (об’єктивізацію актуального стану), потім профільне лікування і власно реабілітація, що сприятиме адаптивній соціалізації. У такому процесі задіяні

батьки (як відповідальні особи за своїх дітей).

П’ята, завершувальна, складова «Ресоціалізація». Досягнення примирення й знаходження порозуміння між жертвою, правопорушником і спільнотою, у якій вони живуть. Оновлене входження індивіда в соціальну систему, використовуючи при цьому нові знання, отриманні уміння і навички. Інтеграція в соціальне середовище відбувається через оволодіння соціально-прийнятими нормами, правилами й цінностями, що стають запорукою успішного функціонування та життєдіяльності.

У рамках усіх складових керуюча роль відводиться саме представникам ювенальної юстиції. Також слід відмітити той факт, що запропонована модель має складну взаємопов’язуючу структуру, так як для її реалізації потрібне залучення інших установ і фахівців, зокрема медичної, психологічної, педагогічної, соціальної ланок, а це потребує розробки регулюючих документів щодо успішної співпраці зазначених установ, зокрема розробки спільних наказів, положень, рекомендацій і інших необхідних керівних документів. Таким чином, на державу покладається функція інформаційного забезпечення й організації інформаційної безпеки захисту документообігу, персональних даних, попередження хакерських атак і таке інше.

Як інструмент практичного вирішення багатьох питань у сфері інформаційної безпеки дитинства буде доцільна реалізація пріоритетних національних проектів «Здорова дитина» та «Якісна освіта», цільових програм, прийняття низки найважливіших 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.

У четвертому розділі –«Медико-психологічні аспекти державного управління інформаційної безпеки особистості»– зазначено, що розгляд впливу травмуючих чинників на психічне здоров’я має велике значення в осмисленні універсального реагування людини на різні дезадаптивуючі впливи і своєчасне проведення медико-психолого-соціальних профілактичних і реабілітаційних заходів.

Досліджено, що 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.

Розглянуто загальні закономірності динаміки психогенних розладів, які виявляються у хворих із пограничними психічними розладами, непатологічні прояви представлені в єдиному ряду психогенних порушень і розглядаються в якості початкового етапу розвитку невротичних симптомів. При ряді умов вони викликають порушення функціональної активності індивідуального бар'єру психічної адаптації. Одне з найбільш частих переживань людей у критичних ситуаціях, яке за надзвичайних впливів може виконувати різні функції, як адаптивну, так і дезорганізуючу психічну діяльність, є емоція тривоги.

Запропонована модель забезпечення інформаційно-психологічної безпеки, що системно поєднує поняття реабілітація-абілітація-компенсація-адаптація та відображає чотири рівні їхньої організації (біологічний, психологічний, соціальний, соціально-психологічний), кожен із яких супроводжується

складовою інформаційного рівня (рис. 7).

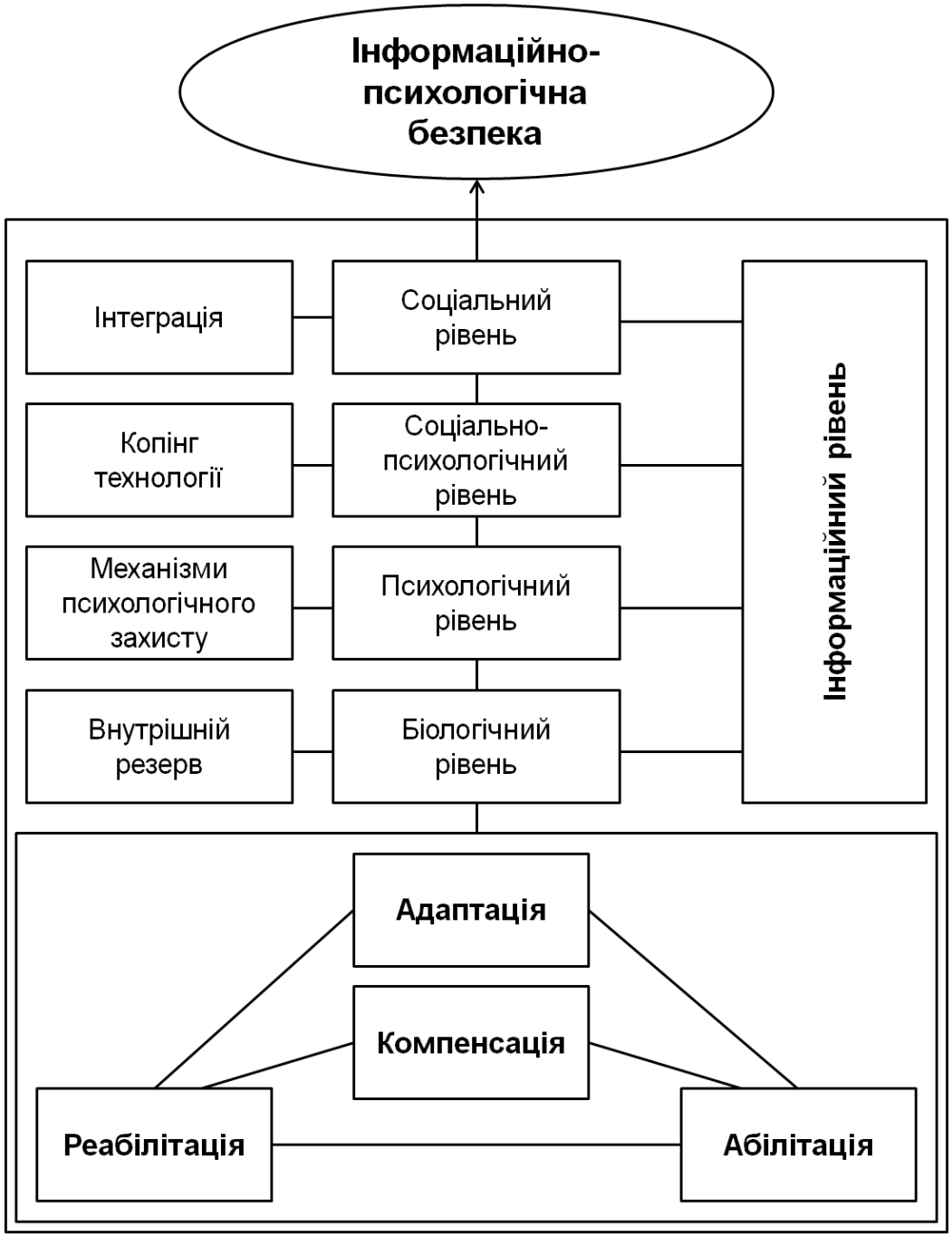

Рис. 7. Модель забезпечення інформаційно-психологічної безпеки

Зазначено, що в зоні військового конфлікту велику роль відіграє інформаційне середовище, що певним чином впливає на психічний стан та психологічне благополуччя населення. 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.

Наводяться результати психодіагностичного дослідження з 2014 по 2019 рр. на базі державного закладу «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України» (ДЗ «НПМ РЦЦ МОЗ України») жителів регіону (дорослих і дітей) із метою виявлення клініко-психопатологічних особливостей розладів психіки та поведінки, що свідчить 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, психотерапію (рис. 8).

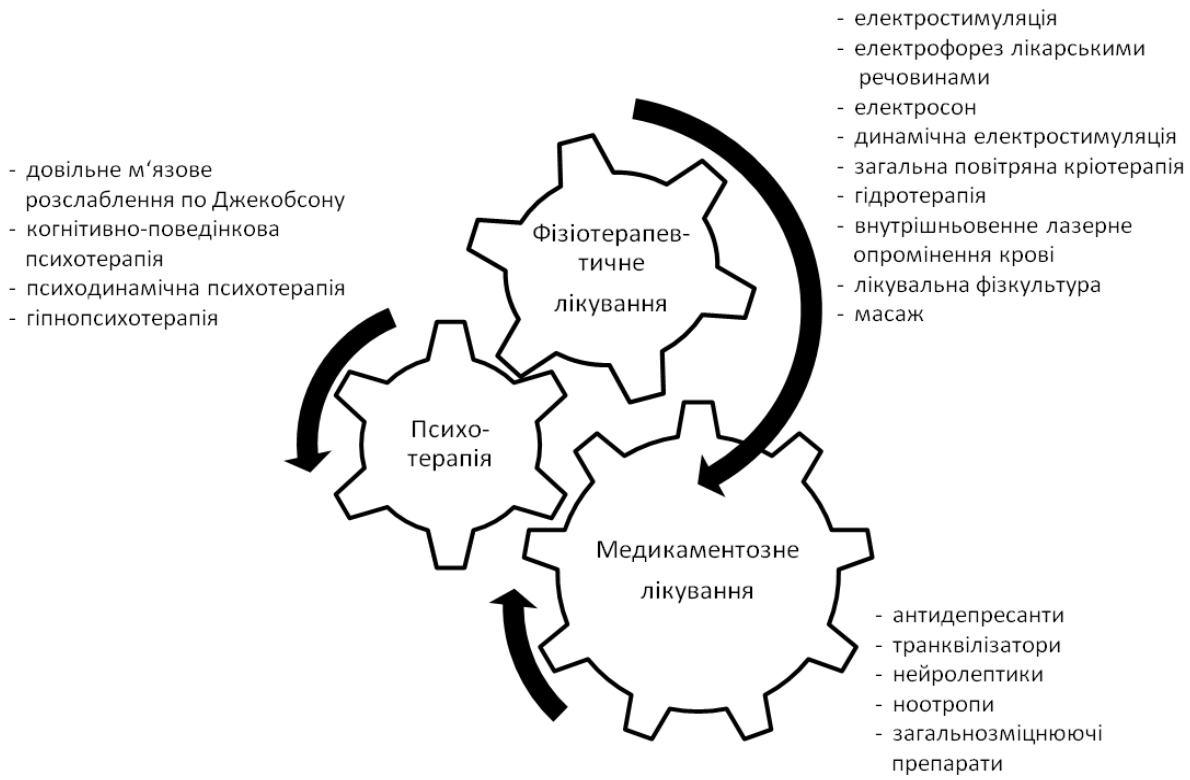

Рис. 8. Комплексна модель реабілітації та абілітації

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.

Реалізація комплексного застосування реабілітаційних заходів здійснюється в амбулаторних умовах, що дає високі показники лікувального (компетентна індивідуалізація кожного окремого випадку, 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.

У п'ятому розділі –«Методологічні аспекти стратегічного управління діяльністю суб'єктів державного управління у сфері інформаційної безпеки»- зазначено, що в Україні назріла об'єктивна необхідність у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але одночасно ефективно захищала б власні українські національні інтереси. Для реалізації останнього найбільш ефективним виступає впровадження стратегічного управління.

Розглянуто й удосконалено зміст поняття «стратегічне управління», що полягає не тільки в умінні моделювати ситуацію, здатності виявляти необхідність змін та розробці самої стратегії із подальшим її втіленням, а більш повно володіти актуальною ситуацією. Перш за все, стратегічне управління – це безперервний процес, що враховує людський потенціал як основу державного управління, при цьому орієнтує діяльність на запити суспільства, гнучко реагує і проводить своєчасні зміни, що відповідають виклику з боку оточення та дають змогу домагатися конкурентних переваг у довгостроковій перспективі, досягаючи при цьому своїх цілей.

Доведено, що ведення стратегічного управління відносно до забезпечення інформаційної безпеки істотно впливає на рішення внутрішньополітичних, зовнішньополітичних та військових конфліктів. 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. Установлено, що для безпеки інформації, що циркулює в органах державної влади, необхідні 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) заходи.

Представлені механізми управління засобами масової інформації даних, що діляться на адміністративно-правові та інформаційні. До першої групи входять механізми реєстрації ЗМІ, правове регулювання інформації, економічні форми впливу, контроль економічної діяльності з боку силових структур.До другої групи – доступ до інформації, присутність на офіційних заходах, доступ до інформації про поточну діяльність органу влади, наближеність до керівників

структур,якість інформації, яка транслюється для ЗМІ. Установлено, що 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.

Розглянуто управління через призму держави, звернено 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 з 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, 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 повинна бути близькою до потреб і запитів простих людей, підконтрольною суспільству, прозорою та ефективною.

Саме функціональний порядок перебуває у найбільш динамічному стані й найбільшевіддзеркалює риси епохи турбулентності. Відомий соціолог-функціоналіст Артур Стінчкомб 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. 9).

В основі функціональної схеми А. Стінчкомба лежать три елементи: 1) основна, гомеостатична змінна **H**, яка знаходиться в рівновазі (об'єкт контролю) і яка власне відображає 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 в залежності від наявних ресурсів і нових умов буде по-іншому впливати на **H**, і яка, у свою чергу, може бути пов'язана з іншими **Hi (**рис. 9).

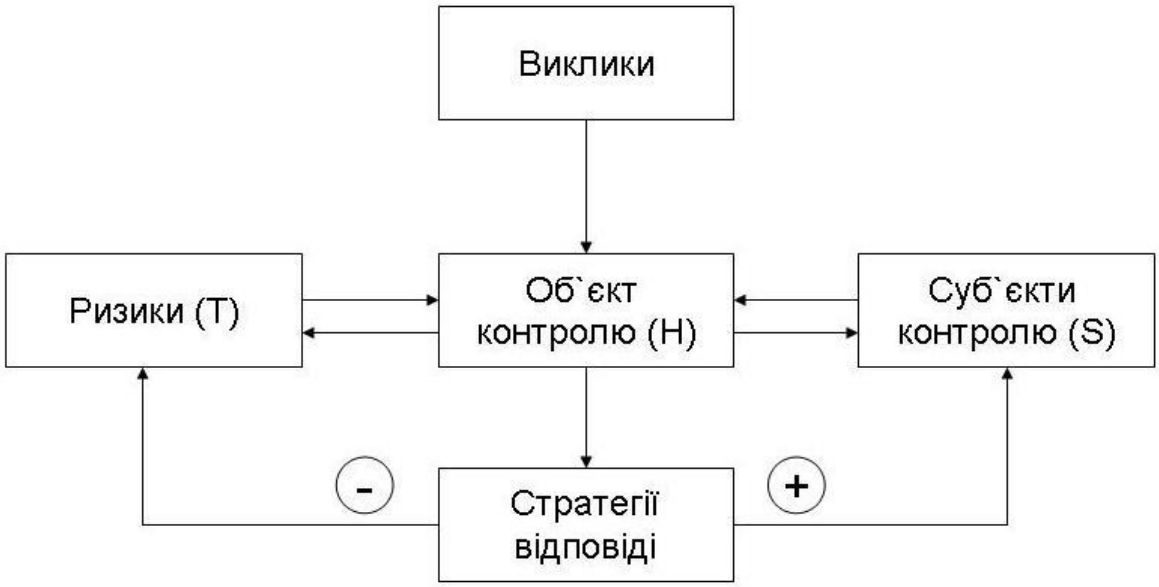

Рис. 9. Модель підтримки рівноваги стану динамічної системи

У розглянутій моделі було зроблено деякі поправки й доповнення. По-перше, у класичній схемі від **Н** до **Т** немає зворотного зв'язку, тільки «негативна» стрілка від **Т** до **Н**. Якщо зв'язати **Н** і **Т** зворотним зв'язком, можна отримати додаткові важелі в поясненні деяких суспільних тенденцій. Чим сильніше тисне **Т**, тим менше значення **Н**, тим більше зусилля докладає **S** для того, щоб відновити значення **H.S** і **Т** формально отримують однаковий статус взаємно протидіючих «сил», пов'язаних прямим і зворотним зв'язком з **Н**. У певному сенсі тут можна говорити про рівнозначність **Т** 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, уводимо елементи «виклики» і «стратегії». Це дає змогу зробити модель більш універсальною. Адже ризики для об’єкта виникають тільки за наявності викликів. А стратегії – це реагування на виклики. Вони можуть бути успішними і вести до зменшення ризиків за рахунок покращення суб’єктів, а можуть бути й негативними – тоді підсилюються ризики.

Сформоване теоретичне підґрунтя дає можливість не тільки за допомогою запропонованої моделі пояснити причини порушення рівноваги стану динамічної системи, а й на її основі визначити заходи щодо її збалансування. Беручи до уваги тему даного підрозділу, наповнення компонентів моделі почнемо з визначення викликів – це інформаційні. Вони є однією із головних характеристик сучасного турбулентного світу. Констатація турбулентності ставить ряд серйозних завдань перед управлінням (суб’єктами контролю згідно є однією із головних функцією держави. Управління – поняття складне й багатогранне, воно залежить від специфіки об’єкта, що у загальному розумінні управління – це цілеспрямований вплив на складну систему. У більш конкретному розумінні управління являє собою діяльність уповноважених

органів, що спрямована на досягнення конкретних завдань за допомогою управлінських методів, способів та функцій.

Розглядаючи управління крізь призму держави, звернемо 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 порядкуі 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. Таке управління має також політичний характер, 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 повинна бути близькою до потреб і запитів простих людей, підконтрольною суспільству, прозорою та ефективною.

При подальшому наповненні моделі очевидним є те, що об'єктом контролю є інформаційна безпека, а ризики – усе те, що її порушує, включаючи такі поняття, як небезпека, загроза, вразливість – між цими концептами, безумовно, існує відмінність, проте в рамках даного контексту не стоїть завдання детального розгляду дефініцій цих понять.

Щодо подальшого наповнення моделі необхідно розглянути кілька уточнюючих моментів. По-перше, інформаційна безпека, завдяки своїй багатогранності, може проявлятися одночасно в кількох змістових компонентах суб'єкта діяльності (управління): об'єкт-мета-результат. По-друге, організаційну діяльність держави в моделі узагальнено можна представити у двох стадіях: перша – створення необхідних засобів та надання їх відповідним суб'єктам, друга – використання засобів суб'єктами у своїй діяльності для вирішення поставлених завдань. У цьому аспекті засоби, як такі, є завданнями й результатом діяльності, спрямованої на досягнення поставленої мети, і перебувають у змістовій єдності із самою діяльністю. Отже,мета-завдання-засоби є останньою ланкою моделі. По-третє, інформаційна, як і будь-яка інша, безпека зумовлюється не лише негативними факторами (ризиками), що можуть посилюватися внаслідок управлінських помилок, а й позитивними та нейтральними процесами, які також потребують цілеспрямованого управлінського впливу: позитивні – підтримання та посилення, нейтральні – трансформації в позитивні (у моделі це показано напрямками «–» і «+»).

Виходячи із системності інформаційної безпеки, можна стверджувати, що її забезпечення є складним, комплексним видом діяльності з надзвичайною структурною розгалуженістю. Сьогодні загальноприйнятого механізму структуризації забезпечення інформаційної безпеки немає. Запропонована модель може бути основою для побудови окремих складових його загальної

структури (рис. 10).

Кожен із напрямків деталізується відповідно до моделі (рис. 10) визначенням мети, завдань і засобів. Докладніше зупинимося на засобах. Із огляду на системність інформаційної безпеки, вони можуть бути: 1) правові; 2) управлінсько-організаційні; 3) інформаційно-аналітичні; 4) психологічного захисту 5) технічного захисту інформації тощо.

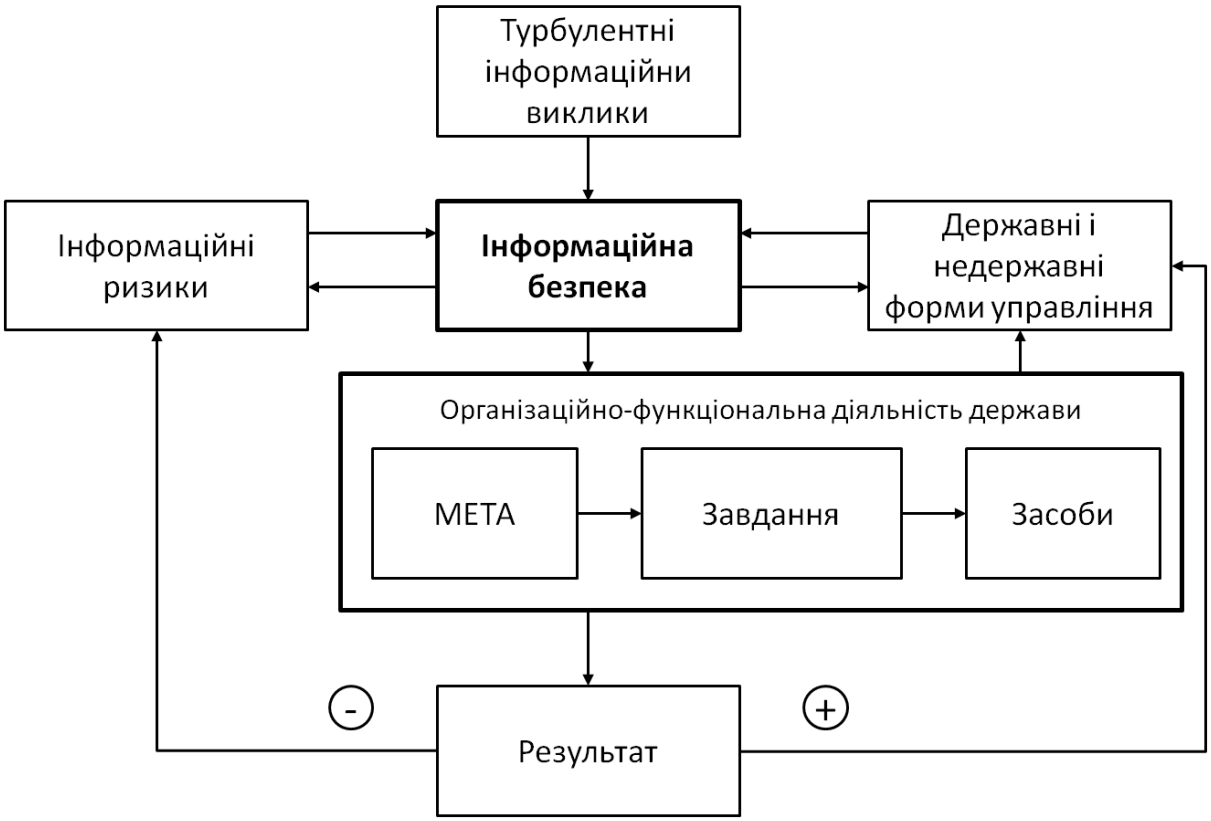

Рис. 10. Модель підтримки динамічної системи забезпечення інформаційної безпеки

Запропонована модель підтримки рівноваги стану динамічної системи забезпечення інформаційної безпеки дозволяє оцінити ризики інформаційних викликів епохи турбулентності та сформувати дієві напрямки державної політики з підтримки рівноваги цієї системи. 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 і незаплановані негативні наслідки їх діяльності; неадекватні стратегії відповіді на виклики; нерелевантність об'єктів контролю, виражених через цінності, принципи і правила умовам, що змінилися.

На основі результатів дисертаційної роботи сформовано концептуальні засади щодо удосконалення державного управління у сфері інформаційної безпеки, зокрема визначені ключові кроки (визначені проблемні сегменти, виокремлено інформаційно-психологічні фактори «інформаційного хаосу»),

змінено основний орієнтир (людиноцентризм), представлено новий зміст, переглянуто принципи, оновлено структуру, удосконалено функціонал (державно-регулюючий, інформаційно-організаційний, медико-психологічний, превентивно-просветницький).

ВИСНОВКИ

Отримані в ході дослідження результати в сукупності розв’язують важливу науково-практичну проблему вдосконалення державного управління спільними діями сил інформаційної безпеки держави при реагуванні на кризові ситуації, що загрожують національній інформаційній безпеці держави впровадженням багаторівневої моделі управління комплексною інформаційною безпекою держави на основі встановлених факторів турбулентності. Результати дослідження дають змогу визначити напрями подальшого розвитку у цій сфері, а також зробити такі висновки.

1. Досліджено теоретико-методологічні засади державного управління інформаційною безпекою в умовах турбулентності, а саме: проаналізовано риси та ознаки епохи турбулентності, суспільний запит на інформаційну безпеку, виділені значущі фактори державної інформаційної безпеки. Доведено, що з позиції системного підходу система забезпечення інформаційної безпеки являє собою відкриту систему зі специфічними і структурними елементами, яка має власні внутрішні зв’язки і зв’язки з навколишнім середовищем, а також функціонує й розвивається під впливом численних факторів. Визначено, що для подолання турбулентності й досягнення керованості, необхідна систематизація та алгоритмічне використання відповідних суспільно-державних механізмів. Доведено, що інформаційна безпека займає ключове місце в системі національної безпеки держави. Проблеми інформаційної безпеки на сьогодні актуалізуються тим, що значно зросла роль накопичення, обробки й 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. І чим вище рівень інтелектуалізації та інформатизації суспільства, тим надійніше його інформаційна безпека. Тому Україні необхідно приділяти своїй національній інформаційній безпеці особливу увагу, оскільки вона є основою визначення найважливіших напрямів і принципів державної політики країни, життєво важливих інтересів особи, держави і суспільства.

2. Відокремлено інформаційно-психологічні фактори турбулентно-політичного й соціально-економічного плану «інформаційного хаосу» та розвинуто понятєво-категорійний апарат державного управління інформаційною безпекою в умовах турбулентності, а саме: дано авторське визначення «епоха турбулентності», що трактується як історичний період, коли частішають і загострюються економічні та соціально-політичні конфлікти з 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. До факторів інформаційного середовища, здатних впливати на психологічну безпеку соціуму, слід віднести якісну та кількісну характеристику інформації (обсяг, справжність, кількість та інше), відповідність характеристик інформації параметрам реципієнтів та установкам навколишнього середовища, наявність у сучасних інформаційних технологіях специфічних елементів, що змінюють психічний стан людини, наявність в інформаційних потоках удосконалених фізичних носіїв інформації, які впливають безпосередньо на фізіологічні носії. Однак інформаційне середовище не єдине джерело ризиків для суспільства, а й сама особистість може бути джерелом формування факторів інформаційно-психологічного ризику, серед яких можна виділити: незрілість і нездатність до фільтрації одержуваної інформації, особистісний конформізм, схильність до маніпулятивних дій іззовні, масове зараження ідеями, функціональні зміни психіки, психоемоційний стрес, фрустрацію, тривожність. Із метою збереження інформаційно-психологічної безпеки людини треба забезпечити постійний контроль і аналіз усіх джерел підвищеного інформаційного ризику, завчасне прогнозування процесів їхнього прояву та оперативне відпрацювання адекватних контрзаходів для відвернення чи мінімізації небажаних наслідків. Розроблена авторська модель забезпечення національної безпеки при об'єктивізації небезпеки збитку у вигляді насильства як на особистісному рівні, так і на державному, що враховує наступні конструкти: превенція; збереження, захищеність, нарощування національних цінностей; усунення збитку, завданого насильством; постпревенційні організаційно-правові заходи для мінімізації можливого збитку, завданого насильством.

3. Досліджено сучасний стан нормативно-правового регулювання інформаційної безпеки та з'ясовано, що нормативно-правові документи з проблематики знаходяться в стадії формування, а тому це несе риси перехідного етапу, визначено проблеми правового забезпечення державного управління інформаційною безпекою. Запропоновані рекомендації щодо покращення функціонування системи інформаційної безпеки органів державної влади, які спрямовані на підвищення ефективності їх діяльності, на захист інтересів держави, а також на захист органів державної влади від несанкціонованого доступу до наявних інформаційних ресурсів. Виділено національні інтереси в інформаційній сфері України, що, у свою чергу, включають інтереси особистості, інтереси суспільства та інтереси держави. Проведено теоретико-правове дослідження правового захисту громадян щодо інформаційної безпеки, яке показало, що 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, що є найважливішим завданням, вирішення якого потребує реалізації ідей правової держави, визначених Конституцією України. Визначено, що 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.

4. Проаналізовано зв'язок між турбулентністю та метаморфозами суспільства, результати яких свідчать про наявність причинно-наслідкового зв’язку. Головною метаморфозою сучасного суспільства є перетворення його в турбулентний стан, де основною ознакою є потокова реальність, і, у силу цього, суспільство пронизане хаотичними, неконтрольованими процесами. Визначено, що інформаційна турбулентність є наслідком синергетики властивостей інформаційного середовища та деструктивним фактором інформаційно-психологічної безпеки як у відношенні до держави і суспільства, так і окремої особистості. Інформаційне насильство поряд із економічним та політичним є системоутворюючим фактором соціального насильства. 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. Доведено, що 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. Характер інформаційних потреб суб'єктів національної безпеки визначає зміст інформаційного забезпечення національної політики, інформаційна безпека повинна бути зорієнтована на забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки всіх суб'єктів сфери інформатизації, бо інформаційне забезпечення національної безпеки являє собою процес задоволення інформаційних потреб суб'єктів національної безпеки.

5. Обґрунтовано аксіологічне бачення інформаційно-психологічної безпеки, що 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; задля чіткої реалізації останнього переглянуто піраміду людських потреб відповідно до сучасних трансформацій інформаційного суспільства, динамізму структури бажань і потягів, що включають у себе більш широкий діапазон потреб сучасної людини. Модернізована піраміда людських потреб уміщує сім рівнів, що утворюють ієрархічну структуру соціальної поведінки людини як основи інформаційно-психологічної безпеки. Доведено, що в певні періоди часу і 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 на різних рівнях інформаційної безпеки. На особистісному рівні важливого значення набуває здатність до адаптації при ознаках збитку психічному здоров'ю. Запропонована модель забезпечення інформаційно-психологічної безпеки, що системно поєднує поняття реабілітація-абілітація-компенсація-адаптація відображає чотири рівні їхньої організації (біологічний, психологічний, соціальний, соціально-психологічний), кожен із яких супроводжується складовою інформаційного рівня.

6. Обґрунтовано комплексний підхід до визначення стратегії розвитку системи інформаційної безпеки в умовах глобалізації, що поєднує функціонування джерел захисту інформації, високий рівень технічного й нормативно-правового забезпечення, конкурентоспроможну професійну компетенцію державних службовців. Важелем такого підходу виступає стратегічне управління, що спрямоване на моделювання ситуації успіху й загроз, здатності виявляти необхідність змін, які відповідають виклику з боку оточення та дають змогу досягати інноваційних переваг, їх гнучко реалізовувати, тим самим формуючи довгострокові перспективи. Таким чином, зазначений підхід орієнтований на створення захищеного середовища для особистості і функціонування інформаційного простору, що сполучає різнорідні засоби захисту інформації, утворюючи інтегровану систему. Перевагою підходу є можливість гарантувати певний рівень безпеки та надійності захисту інформації. Основою дієвої організації й реалізації державної інформаційної політики є формування єдиного інформаційного простору України та її входження до світового інформаційного простору; забезпечення інформаційної безпеки особистості, суспільства й держави; формування демократично орієнтованої масової свідомості; розвиток галузі інформаційних послуг; розширення правового поля регулювання суспільних відносин, у тому числі пов'язаних із отриманням, розповсюдженням і використанням інформації, що, у свою чергу, має сприяти зміцненню зв'язків центру й регіонів, зміцненню цілісності країни.

7. Запропоновано шляхи вирішення проблеми державного управління у сфері забезпечення інформаційної безпеки в умовах турбулентності, які полягають у симбіозі делегування широких повноважень на локальний рівень при належному контролі центру й «культури безпеки» як форми реалізації турботи про себе. Розвиток культури інформаційної 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. На прикладі розгляду інформаційних викликів державі та особистості підтверджена ефективність застосування моделі підтримки рівноваги стану динамічної системи для вироблення дієвих стратегій забезпечення інформаційної безпеки в державному управлінні. Представлена модель спрямована на врівноваження

балансу гомеостатичної змінної різних систем (держава, суспільство, особистість).

8. Аргументованість упровадження нової сучасної концепції розвитку системи державного управління у сфері інформаційної безпеки полягає в зміні орієнтиру, а саме нова концепція повинна бути людиноцентричною, сприяти забезпеченню захищеності і, як наслідок, стійкості основних сфер життєдіяльності (економіки, науки, сфери державного і військового управління, а також суспільної свідомості) від небезпечних, дестабілізуючих і деструктивних інформаційних впливів – на рівні суспільства й держави. У той же час на рівні особистості інформаційна безпека повинна забезпечити захищеність психіки і свідомості людей від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукання до самогубства. Розроблено модель формування системи державного управління у сфері інформаційної безпеки дитини задля покращення становища дітей та удосконалення їх захисту, що вміщує п’ять складових: реінтеграція мікросоціуму, «Comeback» прав і обов'язків, усвідомлення відповідальності, комплексна реабілітація суб'єктів конфлікту, ресоціалізація.

9. Систематизовано та визначено сучасну конфігурацію принципів державного управління у сфері забезпечення інформаційної безпеки громадян. Окреслені принципи представлені наступним змістом: прогнозування і своєчасне виявлення загроз безпеки інформаційних ресурсів, причин і факторів, що сприяють нанесенню шкоди, порушенню його нормального функціонування й розвитку; створення умов функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і нанесення різних видів шкоди; забезпечення механізму й умов оперативного реагування на загрози інформаційної безпеки та прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки; створення умов для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб. Виявлено, що ці принципи повинні ґрунтуватися на загальнонаціональній згоді, що може бути досягнута при кардинальній зміні відношення державних лідерів і інституцій до свого народу в плані відкритості, чесності інформаційних відносин і прозорості своїх дій, так як національна безпека нерозривно пов'язана з діяльністю держави. Тільки вона може, спираючись на свій апарат, владні органи, діяльність яких поставлена в жорсткі рамки і підкріплюється відповідними правовими актами, забезпечити спокій громадян, створити сприятливі умови для їхнього життя та діяльності. Ніякі інші соціальні сили не зможуть виконати цього завдання.

10. Розроблено універсальну модель підтримки рівноваги стану динамічної системи забезпечення інформаційної безпеки, що дозволяє оцінити ризики інформаційних викликів епохи турбулентності та сформувати дієві напрямки державної політики з підтримки рівноваги цієї системи. Основними складовими моделі є об’єкт контролю, суб’єкти контролю, ризики, виклики та стратегії. Індивідуальний аналіз викликів на кожному з рівнів (державному,

регіональному, місцевому, особистісному) дозволяє відповідне планування стратегій до кожного окремого випадку чи ситуації. 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 і 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 і незаплановані негативні наслідки їхньої діяльності; неадекватні стратегії відповіді на виклики; нерелевантність об’єктів контролю, виражених через цінності, принципи і правила умов, що змінилися.

11. Запропоновано концептуальні засади державного управління у сфері інформаційної безпеки при реагуванні на турбулентні явища, що загрожують національній безпеці, які включають державно-регулюючий, інформаційно-організаційний, медико-психологічний, превентивно-просветницький функціонали.

12. Висвітлені концептуальні засади включають сукупність спеціального теоретико-метологічного підґрунтя, а також практичні заходи, засоби, важелі, спрямовані на досягнення основних цілей щодо розбудови надійної інформаційної безпеки держави, а саме: протистояння інформаційним загрозам, мінімізація їх наслідків, якнайшвидшої ліквідації наслідків таких ситуацій та відновлення нормальної життєдіяльності громадян, органів державного управління та місцевого самоврядування, підприємств тощо. Запропонований конструктив полягає у вирішенні завдань, щодо забезпечення інформаційної безпеки як складової національної безпеки держави, а саме: необхідність нормативно-правового регулювання щодо протидії використання інформаційних технологій, які загрожують інтересам держави; необхідність створення економічних передумов для розвитку національних інформаційних ресурсів та інфраструктури, впровадження новітніх технологій в інформаційну сферу. 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.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії:

1. Панченко О.А. Информационно-психологическая безопасность в эпоху турбулентности: монографія. К.: КВИЦ. 2020. 472 с. DOI:10.5281/zenodo.3989790 ISBN 978-617-697-121-4

2. Панченко О.А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект: монографія. К.: КВІЦ. 2020. 332 с. DOI: 10.5281/zenodo.4011826ISBN: 978-617-697-126-9.

3. Панченко О.А. Информационная безопасность ребенка: монографія. К.: КВИЦ, 2016.380 с.

4. Панченко О.А. Інформаційні аспекти трансформації державного управління в умовах турбулентності. *The system of public administration in the context of decentralization of power: Collective monograph*. Riga: Izdevnieciba "Baltija Publishing", 2020. P. 88-110. DOI: 10.30525/978-9934-588-66-2-06.

Особистий внесок здобувача: запропонована авторська модель підтримки рівноваги стану динамічної системи, що дозволяє окреслити ризики викликів епохи турбулентності та сформувати стратегічні напрямки державної інформаційної політики, підтверджено ефективність застосування моделі для вироблення дієвих стратегій забезпечення інформаційної безпеки в державному управлінні на прикладі розгляду інформаційних викликів державі та особистості.

5. Панченко О.А., Банчук Н.В. Информационная безопасность личности: монография. Донецк: ФОП Дмитренко, 2010. 736 с. ISBN 978-966-8965-70-8

Особистий внесок здобувача: запропоновано нові принципові підходи до абілітації і реабілітації людини в умовах інформаційно-психологічного впливу, шляхи підвищення якості життя в його суспільно корисній діяльності, гармонізації суспільних відносин.

6. Панченко О.А., Банчук Н.В. Информационная безопасность личности: монография 2-е изд. испр. К.: КИТ, 2011.672 с. ISBN 978-966-2279-03-0.

Особистий внесок здобувача: проведений теоретичний усебічний аналіз поняття «інформаційна безпека особистості», що включає правові, юридичні, організаційно-технічні та медико-психологічні аспекти, запропоновано ряд базових методів психологічного захисту від маніпуляції в інформаційно-психологічній взаємодії.

7. Панченко О.А., Минцер О.П. Применение информационных технологий в современной реабилитологии: монография.К.: КВИЦ, 2013. 136 с.ISBN 978-617-697-000-2.

Особистий внесок здобувача: проведений теоретичний усебічний аналіз інформаційних процесів у реабілітології і її практичного втілення – реабілітації.Розглянуто три основні напрями: автоматизація діагностичних і лікувальних методик; організаційно-інформаційна підтримка; телереабілітація.

8. Панченко О.А., Банчук Н.В., Пономаренко А.Н., Толстанов А.К., АнтоновВ.Г. Информационные технологии в практике врача: монографія.К.: КВИЦ, 2012. 353 с.

Особистий внесок здобувача: проаналізовані різноманітні аспекти застосування інформаційних технологій у медицині.

9. Панченко О.А. Информационно-психологическая безопасность в условиях гражданского противостояния. *Актуальні дослідження в сучасній і*

вітчизняній екстремальній та кризовій психології: монографія / ред. В.П. Садкового, О.В. Тімченка. Харків. 2017.С. 124-139.

Особистий внесок здобувача: представлена система реабілітації пацієнтів із постстресовими розладами, що включає комплексну діагностику, лікування, реабілітацію, абілітацію та психопрофілактику, запропоновано структурно-функціональну модель інформаційно-психологічної безпеки в умовах громадянського протистояння.

10. Панченко О.А., Кутько И.И. Информационная безопасность личности в чрезвычайных ситуациях. *Посттравматическое стрессовое расстройство:* международная коллективная монография. Под ред. д.мед.н. В.А. Солдаткина. Ростов-на-Дону, 2015. С.199-220.

Особистий внесок здобувача: розглянуто основні питання, що стосуються поняття «інформаційна безпека особистості», запропоновано системні заходи щодо подолання наслідків інформаційного впливу.

Основні статті у наукових фахових виданнях:

11. Панченко О.А. Проблеми правового забезпечення державного управління інформаційною безпекою. *Державне управління: удосконалення та розвиток*. 2019.№ 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1561DOI: 10.32702/2307-2156-2019.11.3.

12. Панченко О.А. Інформаційна безпека держави як елемент соціальної культури. *Аспекти публічного управління.* 2020. № 1. Том 8. С. 58-67. DOI: 10.15421/152006.

13. 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.

14. Панченко О.А. Законотворча діяльність у сфері національної безпеки. *Державне управління: удосконалення та розвиток*. 2020.№ 3. URL: http://www.dy.nayka.com.ua/?op=1&z=1594.DOI: 10.32702/2307-2156-2020.3.7.

15. Панченко О.А. Роль засобів масової інформації в системі державного управління інформаційною безпекою. *Публічне управління та митне адміністрування.*2020. № 1(24). С. 97-102. DOI: 10.32836/2310-9653-2020-1.19.

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

17. Панченко О.А. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України. Серія: Державне управління.* 2019. Вип. 3. URL: http://77.222.145.174/index.php/governance/article/view/296/297

18. Панченко О.А. Засоби масової комунікації як платформа державної інформаційної політики. *Державне управління: удосконалення та*

*розвиток.*2020. № 4. URL: http://www.dy.nayka.com.ua/pdf/4_2020/4.pdf.DOI: 10.32702/2307-2156-2020.4.2.

19. Панченко О.А. Турбулентні соціально-психологічні виклики в системі державного управлінняінформаційною безпекою. *Збірник наукових праць: Теорія та практика державного управління.*2020. Том 1. № 68. С. 210-217. DOI:10.34213/tp.20.01.25.

20. Панченко О.А. Суспільно значущі фактори державної інформаційної безпеки. *Публічне управління і адміністрування в Україні.* 2020. Вип. 16. С.116-120. DOI: 10.32843/2663-5240-2020-16-20

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

Особистий внесок здобувача: переглянуто піраміду людських потреб відповідно до сучасних трансформацій інформаційного суспільства, динамізму структури бажань і потягів, що включають у себе більш широкий діапазон потреб сучасної людини, модернізовано піраміду людських потреб, що вміщує сім рівнів та утворює ієрархічну структуру соціальної поведінки людини як основи інформаційно-психологічної безпеки.

22. Панченко О.А. Провал державної інформаційної політики України. *«Вчені записки» Таврійського національного університету ім. Вернадського. Серія: «Державне управління».* 2020. Том 31(70). № 2. DOI: 10.32838/2663-6468/2020.2/24.

23. Панченко О.А., Гнатенко В.С., Кабанцева А.В. Роль охорони громадського порядку у забезпеченні інформаційної безпеки держави. *Збірник наукових праць: Вісник Національно університету цивільного захисту Серія: «Державне управління».* 2020. Вип. 1(12). С. 265-274. DOI: 10.5281/zenodo.3819249.

Особистий внесок здобувача: проведений теоретичний аналіз законодавчих і нормативно-правових актів у галузі інформаційної безпеки, окреслені варіації інформаційних загроз, надані пропозиції щодо системного забезпечення інформаційної безпеки держави за трьома напрямками – інформаційна безпека особистості, суспільства, держави.

24. Панченко О.А., Кабанцева А.В. Державне регулювання інформаційної складової безпеки дорожнього руху. *Держава та регіони. Серія: Державне управління.* Запоріжжя: Класичний приватний університет, 2020. № 2 (70). С. 184-192. DOI: 10.32840/1813-3401.2020.2.31.

Особистий внесок здобувача: розроблено багаторівневу технологію державного регулювання інформаційної складової безпеки дорожнього руху, яка відображає сукупність державних рішень щодо організації інформації (формування системного підходу), що циркулює на рівні національної системи безпеки дорожнього руху.

25. Панченко О.А., Антонов В.Г. Концептуалізація поняття «інформаційне насилля» в контексті національної безпеки. *Збірник наукових праць: Актуальні*

проблеми державного управління. 2020. № 1 (57). С. 65-73. DOI: 10.34213/ap.20.01.07.

Особистий внесок здобувача: досліджено інформаційне насильство як системне явище та визначені заходи щодо забезпечення національної безпеки в цьому контексті.

26. Панченко О.А., Антонов В.Г. Реабілітація як складова державної політики у сфері інформаційно-психологічної безпеки. *Збірник наукових праць: Теорія та практика державного управління*. 2020. Вип. 2 (69). С. 8-17. DOI: 10.34213/tp.20.02.01.

Особистий внесок здобувача: сформовано теоретичне підґрунтя для розроблення дієвої державної політики щодо організації реабілітаційної допомоги особам, що зазнали збитку психічному здоров'ю.

27. Панченко О.А., Кабанцева А.В., Сердюк І.А. Тривожне очікування людини в епоху турбулентності. *Аспекти публічного управління.* 2020. Том 8. № 2. С. 44-52.DOI: 10.15421/152018.

Особистий внесок здобувача: проведений теоретичний аналіз визначення впливу інформаційного середовища в державі на психологічний стан людини, установлення причинно-наслідкових зв'язків між тривожним передчуттям і турбулентним мисленням в умовах інформаційної небезпеки.

28. Панченко О.А., Пархоменко-Куцевіл О.І., Антонов В.Г. Інформаційні виклики епохи турбулентності в державному управлінні. *Публічне управління та митне адміністрування*: Серія «Державне управління». 2020. № 2 (25). С. 196-204. DOI:10.32836/2310-9653-2020-2.34.

Особистий внесок здобувача: визначено критерії дослідження концепту «епоха турбулентності» та застосування їх в аналізі інформаційних викликів у державному управлінні.

29. Панченко О.А., Кабанцева А.В. Людська психіка в інформаційній небезпеці. *«Вчені записки» Таврійського національного університету ім. Вернадського. Серія: «Державне управління».*2020. Том 31(70). № 3. С. 226-233. DOI: 10.32838/TNU-2663-6468/2020.3/39.

Особистий внесок здобувача: виокремлено негативні прояви впливу сучасного інформаційного простору на людську психіку, розроблено комплекс заходів щодо забезпечення інформаційно-психологічної безпеки особистості та соціуму у державі.

30. Панченко О.А. Інформаційна безпека як складова розвитку суспільних відносин. *Публічне управління і адміністрування в Україні.* 2020. Вип. 17. С. 135-139.URL:DOI: 10.32843/2663-5240-2020-17-25.

31. Панченко О.А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Державне управління та місцеве самоврядування.*2020. Вип. 2 (45). С. 57-63.DOI: 10.33287/102019.

32. Панченко О.А. Інфопандемія в інформаційній гігієні держави. *Право та держава управління*. 2020. № 2. С. 119-126. DOI: 10.32840/pdu.2020.2.18.

Наукові статті у закордонних виданнях:

33. Панченко О.А. Державне управління інформаційною безпекою в турбулентному суспільстві. *World Science*.May 2020. Warsaw, Poland. № 5(57). Vol. 3. P. 4-9. DOI: 10.31435/rsglobal_ws/31052020/7082/.

34. Панченко О.А. Інформаційні технології в забезпеченні державної безпеки. *Science Review.* June 2020. Warsaw, Poland. № 5(32), P. 30-35. DOI: 10.31435/rsglobal_sr.

35. Panchenko O. Panic as a factor of information security threat. Public Administration and Law Review. 2020. Tallinn, Estonia. Issue 2. P. 4-9.DOI: 10.36690/2674-5216-2020-2.

36. Панченко О.А. Інформаційні ризики безпеки дитини в турбулентному інформаційному середовищі. *International academy journal Web of Scholar*.2020.Warsaw, Poland. № 7(49). P. 1-7. DOI:10.31435/rsglobal_wos/30092020/7147.

37. Panchenko, O. Principles of realization of national request for information security. *Public Administration and Law Review.* 2020. № (3). P. 4-11.

Статті в інших наукових виданнях, матеріали конференцій:

38. Панченко О.А., Кабанцева А.В. Державне регулювання інформаційної безпеки дітей. *Тенденції та перспективи розвитку науки і освіти в умовах глобалізації:* збірник наукових праць матеріалів міжнар. наук.-практ. інтернет-конф. (28 лютого 2020 г.)Переяслав, 2020. Вип. 56. С. 39-42.

Особистий внесок здобувача: обґрунтовано необхідність державного регулювання організації інформаційної безпеки дітей в Україні.

39. Панченко О.А., Сердюк І.А. Роль держави в особистісних та суспільних відносинах в епоху турбулентності. *Тенденції та перспективи розвитку науки і освіти в умовах глобалізації:* збірник наукових праць матеріалів міжнар. наук.-практ. інтернет-конф. (28 лютого 2020 г.)Переяслав, 2020. Вип. 56. С. 42-45.

Особистий внесок здобувача: проведений теоретичний аналіз особистісних та суспільних відносин в епоху інформаційної турбулентності.

40. Панченко О.А., Сердюк І.А. Пропаганда та ідеологічна обробка (маніпулювання, інформаційне зомбування) – основи психологічної війни. *Modernization of the educational system: world trend and national peculiarities*: матеріали ІІІ міжнар. наук.конф. (February 21th, 2020) Kaunas, Lithuania, P. 75-79.

Особистий внесок здобувача: проаналізовані основні механізми психологічної війни: пропаганда та ідеологічна обробка (маніпулювання, інформаційне бомбування).

41. Панченко О.А. Види та складові інформаційної безпеки. *ScienceandGlobalStudies:* збірник тез наукових праць ІІ міжнар. наук. конф. (31 березня 2020 р.) Братислава Словаччина, 2020. С.10-13.

42. Панченко О.А., Сердюк І.А. Сучасні уявлення про інформаційну безпеку. *Проблеми модернізації України*: зб. наук. пр. Вип. 10: матеріали конференції *«Розвиток української держави в умовах активізації євро інтеграційних процесів»* (19 березня 2020 р.). К., МАУП. 2020. С. 64-66.

Особистий внесок здобувача: проаналізовані сучасні уявлення про інформаційну безпеку в сфері державного управління

43. Панченко О.А., Гнатенко В.С., Малєєва А.М. Інформаційна безпека як складова економічної безпеки держави. *Проблеми модернізації України:* зб. наук. пр. Вип. 10: матеріали конференції *«Розвиток української держави в умовах активізації євро інтеграційних процесів»* (19 березня 2020 р.). К., МАУП. 2020. С. 20-23.

Особистий внесок здобувача: розглянуто інформаційну безпеку як складову економічної безпеки держави.

44. Панченко О.А. Информационные аспекты психологической безопасности в турбулентное время. *Интеграционное развитие личности и общества: психологическое и социологическое измерение:* материалы II междун. научно-практ. конф. (12 июня 2020 г.) Одесса, 2020. С. 195-199.

45. Панченко О.А., Сердюк І.А. Інформаційно-психологічна безпека людини в умовах турбулентного розвитку.*Україна 2030: публічне управління для сталого розвитку:* матеріали щоріч. міжнар. наук.-практ. конф. (Київ, 2020 р.): у 3 т. / за заг. ред. А. П. Савкова, М. М. Білинської, О. М. Петроє. Київ: НАДУ, 2020. Т. 1. С. 98-100.

Особистий внесок здобувача: обґрунтовано постійний інформаційно-психологічний вплив на особистість в умовах турбулентного розвитку, установлено ряд факторів інформаційного середовища, здатних впливати на психологічну безпеку соціуму.

46. Гнатенко В.С., Панченко О.А., Малєєва А.М. Економічні ризики в умовах інформаційної турбулентної держави. Україна 2030: публічне управління для сталого розвитку: матеріали щоріч. міжнар. наук.-практ. конф. (Київ, 2020 р.): у 3 т. / за заг. ред. А.П. Савкова, М.М. Білинської, О.М. Петроє. Київ: НАДУ, 2020. Т. 1. С. 155-157.

Особистий внесок здобувача: визначено економічні ризики в умовахінформаційної турбулентності держави

47. Панченко О.А. Психологические аспекты турбулентности информационной среды. *Причорноморські психологічні студії*. Одеса. 2017. Вип. 1. С. 3-7.

48. Панченко О.А., Антонов В.Г. Понятие «Турбулентность» в системе информационно-психологической безопасности личности. *Медико-психологические вызовы современности*: сборник тезисов научно-практ. конф. с междунар. участием (2 ноября 2017 г.) Константиновка: Контраст, 2017. С. 69-73.

Особистий внесок здобувача: *запропонована структурно-функціональна модель забезпечення інформаційно-психологічної безпеки в причинно-наслідковому зв'язку з інформаційно-психологічною турбулентністю.*

49. Панченко О.А. Психологическая турбулентность в условиях информационной войны.*Становлення та розвиток особистості в умовах інформаційної війни:* матеріали наук.-практ. конф. (2 березня

2018 р.) Київ:Таврійський національний університет імені В.І. Вернадського, 2018. С. 148-151.

50. Панченко О.А., Антонов В.Г. Информационные угрозы как фактор турбулентного мышления. *Реалізація тривоги в психічні та соматичні розлади в 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 О.А. Панченка. «Контраст», 2018. С. 108-115.

Особистий внесок здобувача: *розкрито сутність поняття «турбулентність мислення» як способу адекватної відповіді на інформаційні загрози.*

51. Антонов В.Г. Панченко О.А. Турбулентность – как угроза надежности системы «человек-машина».*Інформаційні системи та технології в медицині*: збірник наукових праць II міжнар. наук.-практ. конф. (ISM-2019) (28-29 листопада 2019 р.) Харків: Нац. аерокосм. ун-т ім. Жуковського «Харків.авіац. ін.-т», 2019. С. 28-30.

Особистий внесок здобувача: *виявлено турбулентні загрози в системі «людина-машина» та запропоновано шляхи підвищення надійності її роботи.*

52. Панченко О.А. Турбулентність мислення в структурі інформаційно-психологічної безпеки особистості. *Психологія і особистість.* Київ – Полтава. 2019. № 1 (15). С. 41- 60.

53. Панченко О.А. Информационная безопасность в эпоху турбулентности. *Інформаційні системи та технології в медицині*: збірник наукових праць II Міжнар. наук.-практ. конф. (ISM-2019) (28-29 листопада 2019 р.) Харків: Нац. аерокосм.ун-т ім. Жуковського «Харків.авіац. ін.-т», 2019. С. 18-19.

54. Панченко О.А., Пономарьова Г.В. Постстресові розлади в умовах інформаційної та гібридної війни. Матеріали *XVI з`їзду Всеукраїнського лікарського товариства* Кам`янець-Подільський, (28 вересня – 1 жовтня 2017 року). Кам`янець-Подільський, 2017. С.131-132.

Особистий внесок здобувача: *розроблено психодіагностичний комплекс, що дозволяє своєчасно діагностувати властивості особистості, а також відстежувати їхню динаміку в процесі проведення лікувальних і реабілітаційних заходів.*

55. Панченко О.А. Постстресові розлади в умовах інформаційно-психологічної турбулентності. *Психосоціальна підтримка осіб з травмою війни: міжнародний досвід та українські реалії:* матеріали всеукраїнської науково-практичної конференції (Маріуполь, 28 лютого 2018 р.). Маріуполь, 2018. С.50-52.

56. Панченко О.А. Постстресові розлади в умовах громадянського протистояння. *Український вісник психоневрології*. 2017. Т. 25, Вип.1. С. 139-140.

57. Кутько И.И., Панченко О.А., Линев А.Н., Линева Р.С. Актуальные проблемы ПТСР у военнослужащих в современных условиях.*Український вісник психоневрології*. 2015. Т. 23, Вип. 2 (83). С. 112.

Особистий внесок здобувача: *виявлено посттравматичний стресовий розлад у військовослужбовців за сучасних умов.*

58. Панченко О.А. Правовой аспект информационной безопасности.*Психологічні технології в екстремальних видах діяльності*: матеріали VI міжнародної науково-практичної конференції. (20-21 травня 2010р.) Донецьк: Донецький юридичний інститут ЛДУВС ім. Е.О. Дідоренка, 2010. С. 191-194.

59. Панченко О.А., Банчук Н.В. Информационная безопасность личности в современном информационном обществе. *Український журнал телемедицини та медичної телематики*. 2012. Т. 10, № 1. С. 106-107.

Особистий внесок здобувача: *досліджено поняття «турбулентність» у різних аспектах вивчення й забезпечення інформаційної безпеки особистості.*

60. Панченко О.А., Панченко Л.В. Информационная культура и безопасность личности в условиях интернет-социализации. *Соціалізація і ресоціалізація особистості в умовах сучасного суспільства:* матеріали IV міжнар. наук.-практ. конф. (7-9 листопада 2014 р.) Київ, 2014. С. 162-165.

Особистий внесок здобувача: *проаналізовано сутність взаємозв'язку інформаційної безпеки та інформаційної культури особистості в умовах становлення інформаційного суспільства, наведено визначення понять інформаційної безпеки та інформаційної культури, характеристики їхніх складових та причинно-наслідкових зв'язків між ними.*

61. Панченко О.А. Информационно-психологическая безопасность в условиях гражданского противостояния. *Актуальні дослідження в сучасній і вітчизняній екстремальній та кризовій психології:* монографія / ред. В.П. Садкового, О.В. Тімченка. Харків. 2017.С. 124-139.

62. Панченко О.А., Антонов В.Г., Гуменюк В.В. Информационные технологи в медико-психологическом контроле для обеспечения безопасности дорожного движения.*Медико-психологические вызовы современности*: сборник научно-практ.конф. с междунар. участием (2 ноября 2017 г.) Константиновка: Контраст, 2017. С. 74-78.

Особистий внесок здобувача: *досліджено роль та рівень застосування інформаційних технологій у медико-психологічному контролі, визначено складові інформаційних технологій у системі охорони здоров'я.*

63. Панченко О.А., Цапро Н.П., СимоненкоЕ.Б. Роль психогенных факторов в возникновении функциональных расстройств у детей и подростков. *Современные проблемы и пути их решения в науке, транспорте, производстве и образовании 2010*: сб. материалов междунар. научно-практ. конференции. (20-27 декабря 2010г.) Одесса: Черноморье, 2010. Т. 22. С. 35-37.

Особистий внесок здобувача: *визначено психотравмуючі соціально-психологічні фактори, що призводять до формування психічних та психосоматичних розладів у дітей та підлітків, постраждалих унаслідок Чорнобильської катастрофи.*

64. Панченко О.А., Симоненко Е.Б., Зарубайко А.В., Цапро Н.П.Воздействие информационной среды на психическое и соматическое

здоровье ребенка. *Актуальні проблеми психології*: збірник наукових праць Інституту психології ім. Г.С.Костюка НАПН України. Житомир: Вид-то ЖДУ ім. І. Франка, 2015. Т. VI, Вип. 10. С. 100-107.

Особистий внесок здобувача: *розроблено комплекс психодіагностичних методик, що дозволяє виявити емоційні порушення в умовах інформаційного середовища.*

65. Панченко О.А., Банчук Н.В., Антонов В.Г., Жуков А.П. Концептуальная модель информатизации реабилитационного центра. *Інформаційні системи та технології в медицині*: збірник наукових праць II міжнар. науково-практична конференція (ISM-2019) (28-29 листопада 2019 р.) Харків: Нац. аерокосм.ун-т ім. Жуковського «Харків.авіац. ін.-т», 2019. С. 52-54.

Особистий внесок здобувача: *сформована концептуальна модель інформатизації реабілітаційного центру в умовах позначених «чинників успішності».*

66. Информатизация реабилитационного процесса: сборник научных работ / Под. общ. ред. д.мед.н., проф., Заслуженного врача Украины О.А. Панченко. Киев: КВИЦ, 2013. 161 с.

Особистий внесок здобувача: виокремлено проблеми інформаційного забезпечення медичних закладів на сучасному етапі, застосування інформаційних технологій у діагностиці та реабілітації пацієнтів із різною патологією.

67. Панченко О.А., Сердюк І.А. Інформаційна державна політика на шляху цифровізації. *Публічне управління у цифровому суспільстві:* матеріали науково-практичної конференції (Дніпро, 25 червня 2020 г.). 2020. С. 107-109.DOI:10.15421/152053

Особистий внесок здобувача: виявлено завдання інформаційної державноїполітики на шляху цифровізації.

АНОТАЦІЯ

Панченко О.А. Державне управління інформаційною безпекою в епоху турбулентності. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора наук із державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. – Національний університет цивільного захисту України. – Харків, 2020.

Робота присвячена сучасним проблемам державного управління інформаційною безпекою при реагуванні на кризові ситуації та турбулентні явища, що загрожують національній інформаційній безпеці держави. Визначені ризики й загрози інформаційної та психологічної безпеки особистості, суспільства, держави. Запропоновані дієві шляхи щодо забезпечення інформаційної безпеки на основі встановлених факторів турбулентності.

У дисертації узагальнено теоретико-методологічні засади державного управління інформаційною безпекою в умовах турбулентності. Доведено, що

інформаційна безпека займає ключове місце в системі національної безпеки держави. Відокремлено інформаційно-психологічні фактори турбулентно-політичного й соціально-економічного плану «інформаційного хаосу» та розвинуто поняттєво-категорійний апарат державного управління інформаційною безпекою в умовах турбулентності, надано авторське визначення «епоха турбулентності».

Установлені методологічні аспекти стратегічного управління діяльності суб'єктів державного управління у сфері інформаційної безпеки, які спрямовані на підвищення ефективності діяльності органів державної влади, на захист інтересів держави, а також від несанкціонованого доступу до наявних інформаційних ресурсів. Представлено аксіологічне бачення інформаційно-психологічної безпеки, що полягає в забезпеченні психологічного благополуччя особистості та направлено на мінімізацію різноманітних ризикових факторів формування і функціонування адекватної інформаційно-орієнтовної основи суб'єктивно-особистісних відносин до навколишнього світу і самої себе.

Обґрунтовано комплексний підхід до визначення стратегії розвитку системи інформаційної безпеки в умовах глобалізації, що поєднує функціонування джерел захисту інформації, високий рівень технічного й нормативно-правового забезпечення, конкурентоспроможну професійну компетенцію державних службовців. Запропоновано концептуальні засади державного управління у сфері інформаційної безпеки при реагуванні на турбулентні явища, що загрожують національній безпеці, які включають сукупність спеціальних практичних заходів, засобів, важелів, спрямованих на досягнення головної мети якнайшвидшої ліквідації наслідків таких ситуацій та відновлення нормальної життєдіяльності громадян, органів державного управління та місцевого самоврядування, підприємств тощо. У дослідженні вперше розроблено модель підтримки рівноваги стану динамічної системи забезпечення інформаційної безпеки, що дозволяє оцінити ризики інформаційних викликів епохи турбулентності та сформувати дієві напрямки державної політики з підтримки рівноваги цієї системи. Висвітлено пропозиції державного регулювання щодо організації медико-психологічної допомоги постраждалим унаслідок негативного інформаційного впливу. Створена модель забезпечення інформаційно-психологічної безпеки, що системно поєднує поняття реабілітація-абілітація-компенсація-адаптація та відображає чотири рівні їхньої організації (біологічний, психологічний, соціальний, соціально-психологічний), кожен із яких супроводжується складовою інформаційного рівня. На основі дослідження інформаційних ризиків безпеки дитини в турбулентному середовищі розроблено модель формування системи державного управління у сфері інформаційної безпеки дитини.

У дисертації закладено не тільки теоретичну основу для розробки дієвої державної політики щодо організації реабілітаційної допомоги особам, які мають збитки психічному здоров'ю, а й визначено практичні кроки її реалізації.

Ключові слова: державне управління, інформаційна безпека, епоха турбулентності, національна безпека, інформаційне середовище, інформаційна політика держави, інформаційно-психологічна безпека, правове забезпечення безпеки, завдання правового забезпечення, правове регулювання безпеки, державне управління інформаційною сферою, реабілітація, абілітація.

SUMMARY

Panchenko O.A. Government control of the information security in the era of turbulence. –*Qualifying scientific work on the rights of the manuscript.*

Doctoral candidate's thesis of government control by specialty 25.00.05 – public administration in the field of the state safety and protection of a public order. – National University of Civil Defense of Ukraine. – Kharkiv, 2020.

The work is devoted to modern problems of state management of information security in response to crises and turbulent phenomena that threaten the national information security of the state. Risks and threats of information and psychological security of a person, society and the state have been defined. Effective ways to ensure information security based on established turbulence factors have been proposed.

The dissertation generalizes the theoretical and methodological principles of the government control of information security under conditions of turbulence. It has been proved that information security occupies a key place in the national security system of the state. The information-psychological factors of the turbulent-political and socio-economic plan of "information chaos" have been separated and the conceptual-categorical apparatus of the government control of information security under the conditions of turbulence have been developed and the author's definition "epoch of turbulence" has been given.

The methodological aspects of strategic management of public administration in the field of information security, which are aimed at improving the efficiency of public authorities, to protect the interests of the state, as well as from unauthorized access to available information resources have been defined.An axiological vision of information and psychological security has been presented, which consists of ensuring of the individual's psychological well-being and aims to minimize various risk factors for the formation and functioning of an adequate information-oriented basis of subjective-personal relations to the world and oneself.

The complex approach to definition of system development strategy of information security under the conditions of globalization which combines functioning of information protection sources of, a high level of technical and normative-legal maintenance, competitive professional competence of public officers has been proved. The conceptual provisions of government control in the sphere of information security in response to turbulent phenomena that threats the national security, which include a set of special practical measures, tools, levers aimed at achieving the main goal of eliminating the consequences of such situations and restoring normal life of citizens,

public administration and local self-government, enterprises, etc. In this study for the first time, a model for maintaining the balance of the dynamic information security system, which allows to assess the risks of information challenges of the turbulent era and to form effective directions of public policy to maintain the balance of this system, has been developed. The proposals of state regulation on the organization of medical and psychological care for victims of negative information impact have been highlighted. A model of information and psychological security has been created, which systematically combines the concepts of rehabilitation-abilitation-compensation-adaptation and reflects four levels of their organization (biological, psychological, social, socio-psychological), each of which is accompanied by an information level component. Based on the study of information risks for child's safety in a turbulent environment, a model of forming a system of public administration in the sphere of child information security has been developed. The dissertation builds not only a theoretical basis for the development of an effective state policy for the organization of rehabilitation care for persons with mental health problems, but also identifies practical steps for its implementation.

Key words:government control, information security, epoch of turbulence, national security, information environment, information policy of the state, information and psychological security, legal support, legal tasks, legal regulation of security, government control of information sphere, rehabilitation, abilitation.

Відповідальна за друк *Пархоменко-Куцевіл О.І.*

Підписано до друку 20.09.2020 р.
Формат 60х84 $^{1}/_{16}$. Обл.-вид. арк. 0,9.
Гарнітура Таймс. Тираж 100 прим.

Віддруковано з оригінал-макета в друкарні ФОП Леонов Д.С.
61023, м. Харків, вул. Весніна, 12, тел. (057) 717-28-80.