

ПСИХОЛОГІЯ

УДК 159.9

DOI: <https://doi.org/10.17721/1728-2217.2022.49.13-21>В. Алещенко, д-р психол. наук, проф.
avi1953@ukr.net
ORCID ID 0000-0003-1560-7318

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

**ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ОСОБИСТОСТІ
В УМОВАХ ГІБРИДНОЇ ВІЙНИ**

Досліджено актуалізацію проблеми інформаційно-психологічної безпеки особистості в умовах гібридної війни. Наведено нормативно-правові основи інформаційної безпеки як важливої складової безпеки держави. Проаналізовано поняття безпека, національна безпека, інформаційна безпека, інформаційно-психологічна, психологічна безпека. Розкрито основні критерії психологічної безпеки особистості з урахуванням інформаційного впливу. Розглянуто зовнішні та внутрішні фактори психологічних механізмів інформаційного впливу на особистість, суспільство, державу в цілому. Визначено основні суб'єкти та об'єкти інформаційно-психологічного впливу. Актуалізовано питання трансформації психологічної безпеки особистості як наслідку тривалого інформаційно-психологічного впливу. Наведено структурно-функціональну модель інформаційно-психологічної безпеки особистості. Узагальнено та розглянуто теоретико-прикладні аспекти роботи з військовослужбовцями в умовах деструктивних інформаційних впливів, що вимагають обов'язкового врахування органами військового управління ЗСУ, для забезпечення ефективності роботи з військовослужбовцями під час вирішення завдань за призначенням. Виокремлено напрями інформаційно-психологічних атак проти України та наведено класифікацію інформаційно-психологічних загроз. Визначено негативні наслідки інформаційно-психологічного впливу на психіку та наведено ефективні способи протистояння негативному впливу інформаційних потоків. Підкреслено, що підвищенню інформаційно-психологічної безпеки особистості сприяють контроль інформаційного середовища, навчання населення основам медіаграмотності, проведення заходів щодо захисту інформаційного середовища від зовнішніх негативних впливів тощо.

Ключові слова: інформаційний простір, інформаційно-психологічна безпека, інформаційно-психологічний вплив, морально-психологічний стан, інформаційно- психологічний стрес.

Постановка проблеми. Сучасна епоха характеризується появою війн нового покоління, що мають основною метою не фізичне знищення противника, а досягнення політичних, економічних та соціальних цілей без збройного протистояння військових формувань. Настала епоха "гібридних" війн, у яких пряме збройне втручання не є основною метою, а використовуються нові форми і методи, спрямовані на підірив могутності противника "зсередини". Погоджуємося з висловом К. Клаузевіца – "будь-яка епоха має свої власні війни". Сучасна епоха – не виняток.

Вигідне геополітичне положення України та ряд інших чинників обумовлюють наявність політичних, економічних та інших інтересів з боку сусідньої держави, що характеризується безперервним інформаційно-психологічним впливом на всі сфери діяльності нашої держави. У цьому контексті проблеми забезпечення інформаційно-психологічної безпеки (ІПБ) особистості в умовах гібридної війни з боку Російської Федерації (РФ) набувають усе більшої значущості. З огляду на зовнішні та внутрішні загрози інформаційний простір України став насиченим негативними подіями, що ще більше пригнічує громадян, впливає і на морально-психологічний стан особового складу Збройних Сил України (ЗС України). Повільний розвиток системи стратегічних комунікацій і недосконалість інформаційної політики держави ускладнюють боротьбу проти гібридних загроз, які увійшли в активну фазу. За цих умов важливу роль в ефективності забезпечення національної безпеки держави виконує інформаційно-психологічна безпека особистості, суспільства, держави.

Сьогодні особистість живе і функціонує в інформаційному світі. Проявом гібридної війни в інформаційно-психологічній сфері є постійний вплив засобами вербальної та невербальної комунікації на свідомість і підсвідомість особистості. Загальним джерелом зовнішніх

загроз є інформаційне середовище, яке різними методами подає спотворену інформацію щодо навколишньої дійсності, надає неправдиву інформацію, змінює поведінку індивіда, соціальних груп щодо себе самих, соціуму та держави. Усе це має реальну загрозу для розвитку особистості й суспільства загалом. Маніпулювання свідомістю людей, використання різноманітних засобів і технологій інформаційно-психологічного впливу на них стало досить звичним явищем. В інформаційних атаках на громадян України беруть участь професійні команди, фахівці, які знають, як можна розхитати свідомість особистості і як впливати на її психічний стан, розмивати традиційні духовно-моральні цінності.

Масштабність і потужність сучасних гібридних впливів на психіку особистості актуалізують порушену проблему. Отже, вживання заходів щодо стримування та протидії проявам негативних інформаційно-психологічних впливів як складової гібридної війни на свідомість та підсвідомість особистості, розуміння цих загроз для безпеки особистості, механізмів їхньої дії та можливостей захисту є надзвичайно актуальною проблемою і потребує негайного вирішення не лише на теоретичному рівні. Тому науковий аналіз порушеної проблематики сприятиме кращому розумінню загроз та викликів для України.

Аналіз останніх досліджень і публікацій. Українські науковці видали ряд наукових публікацій, присвячених різним аспектам означеної проблематики (В. Алещенко, М. Корольчук, О. Матеюк, В. Мулява, В. Осьодло, Г. Почепцова, І. Приходько, О. Сафін, В. Телелим, О. Хайрулін, О. Хміляр, О. Юдін). Серед зарубіжних авторів, що займаються цими проблемами, слід зазначити роботи М. Бангеманна, Д. Волгогомова, Є. Доценка, П. Дракера, О. Караяні, Р. Катца, Д. Лайона, В. Лісичкіна, М. Маклюєна, А. Манойла, Дж. Мартіна, С. Расторгуєва, Д. Рісмана, Т. Стоуньєра,

© Алещенко В., 2022

І. Сиромятникова, Д. Тапськотта, Е. Тоффлера, Х. Шрадера та ін. Цю проблему і ми проаналізували в роботах [1, 2]. У працях вищезазначених науковців інформаційна безпека досліджувалась як складова національної безпеки, її невід'ємний компонент. Однак питанню характеристики інформаційно-психологічної безпеки особистості в умовах гібридної війни, на нашу думку, приділялось недостатньо уваги.

Помітним явищем у дослідженні сучасних війн стали монографії "Світова гібридна війна: український фронт" [3] та "Кремлівська агресія проти України: роздуми в контексті війни" [4], у яких автори розглядають витoki і передумови російської гібридної війни проти України, її прояви на гуманітарному і внутрішньополітичному фронтах та наголошують, що її мета – "деморалізувати громадян, підірвати їхню лояльність, посягти серед них зневіру й паніку, спричинивши у такий спосіб розлад та руйнацію всіх соціальних інституцій, у тому числі інституції державності" [4, с. 19].

Сьогодні існують також альтернативні погляди на інформаційно-психологічну безпеку. На думку фахівців Johns Hopkins University & Imperial College London існує когнітивна безпека людської свідомості. Її мета полягає в оцінці не лише того, що думає людина, а й того, як вона думає і діє. За успішної реалізації заходів когнітивної безпеки реалізується індивідуальна та групова емоційна стійкість [5].

Мета дослідження – виявлення негативних проявів впливу гібридних форм і способів сучасного інформаційного простору на людську психіку та формулювання відповідних пропозицій щодо забезпечення інформаційно-психологічної безпеки особистості.

Виклад основного матеріалу дослідження. Аналіз досліджень зарубіжних і вітчизняних науковців показує, що достатньо обґрунтованим є висновок, – до змісту інформаційної безпеки долучаються і проблеми ІПБ особистості. Проблеми захисту психіки, персональних даних, фінансових інструментів людини в контексті боротьби з інформаційними загрозами, кіберзлочинами є важливим завданням як для кожної людини, так і в цілому для держави. Серед дослідників поширено підхід – інформаційно-психологічну безпеку особистості розглядати у сфері *інформаційної безпеки* (ІБ). Проте, на нашу думку, доцільним буде її виокремлення від інформаційної в самостійний напрям та необхідність активної розробки зазначеної проблематики. Варто побудувати принципову модель ІБ особистості в представленому вигляді (рис. 1).

Основними компонентами концептуальної моделі ІБ особистості можна вважати: об'єкт загрози – особистість (зазіхання на життя, здоров'я, свободу, загрози за відповідними властивостями інформації); джерела загроз; напрями захисту (нормативно-правовий, організаційний, інженерно-технічний); способи захисту; способи захисту об'єкта загроз – усі інформаційні ресурси держави, суспільства або громадян, які підлягають захисту згідно з визначеною політикою безпеки та чинним законодавством.

Розглядаємо сутність безпеки особистості як найвищу цінність держави, як можливість задоволення

потреб, функціонування та розвитку особистості, відсутність загроз життєво важливим інтересам людини: її життю, здоров'ю, добробуту, свободи, її гідності. Своєчасним вважаємо сформулювати ключові поняття, базуючись на методології як українських, так і зарубіжних фахівців.

Тлумачний словник української мови [6] визначає безпеку як стан, коли кому-небудь або чому-небудь ніщо не загрожує. Рівень особистої безпеки залежить насамперед від самої людини: як вона вміє передбачати небезпеки й уникати їх, раціонально діяти в небезпечній ситуації, від її характеру й особистих якостей. Аналіз змісту терміна "безпека" показує, що в суспільній свідомості це поняття асоціюється не так з "відсутністю загроз", як зі станом, почуттями та переживаннями людей. Загалом поняття "безпека" отожднюється зі станом особистості та почуттям відсутності тривоги чи стурбованості, упевненості, стабільності.

Визначення нашої теми нас на детальний розгляд поняття "національна безпека", який, на нашу думку, охоплює як рівноправні складові терміни "державна безпека", "інформаційна безпека", "інформаційно-психологічна безпека особистості", "психологічна безпека особистості". Очевидно, що **національна безпека** – це надзвичайно складна багаторівнева функціональна система, у якій безперервно відбуваються процеси взаємодії та протидії життєво важливих інтересів держави, суспільства та особистості із загрозами цим інтересам – і внутрішніми, і зовнішніми [7] або реалізованість життєво важливих інтересів людини, суспільства та держави в різних сферах їхньої життєдіяльності в умовах впливу внутрішніх і зовнішніх загроз [8].

Інформаційна безпека – важлива складова національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави. Слід зазначити, що інформаційна безпека є не лише самостійною складовою національної безпеки, але й складовою інших сфер національної безпеки держави, спрямованою на забезпечення національних інтересів у цих сферах [9]. Згідно зі ст. 17 Конституції України забезпечення інформаційної безпеки держави стоїть на одному рівні із захистом суверенітету й територіальної цілісності України, забезпеченням її економічної безпеки як найважливішими функціями держави [10].

Інформаційна безпека особистості – це стан людини, у якому його особистості не може бути завдано істотної шкоди шляхом здійснення впливу на навколишній інформаційний простір. Під інформаційно-психологічною безпекою розуміють стан захищеності громадян, окремих груп та соціальних верств, масових об'єднань людей і населення загалом від негативних інформаційно-психологічних впливів.

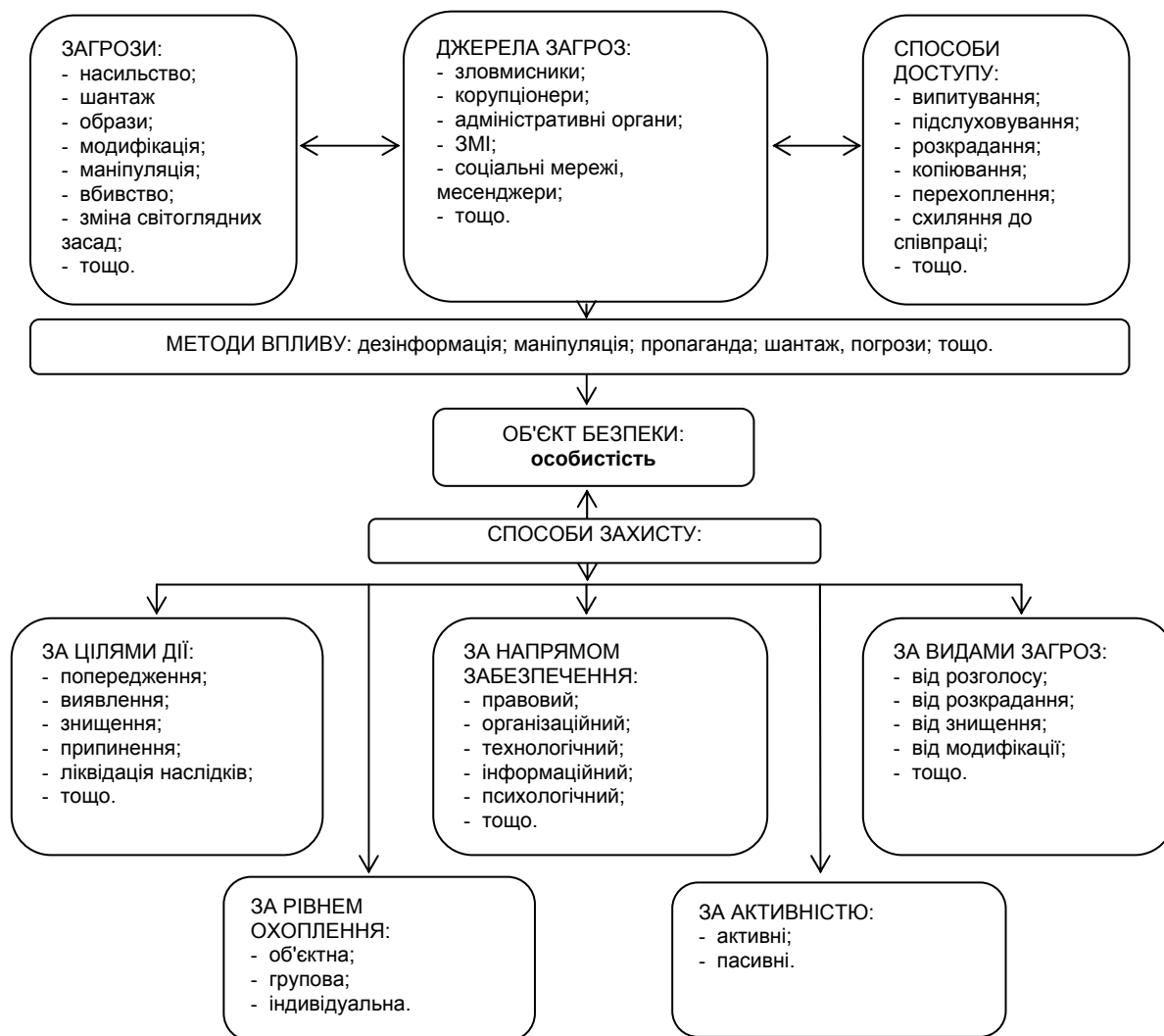


Рис. 1. Концептуальна модель інформаційної безпеки особистості

Отже, інформаційна безпека особистості, суспільства та держави характеризується ступенем їхньої захищеності, стійкістю головних сфер життєдіяльності щодо небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйнятим є таке визначення інформаційної безпеки як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері [2].

Під психологічною безпекою особистості розуміємо позитивне самовідчуття людини, її емоційне, інтелектуальне, особистісне та соціальне благополуччя в конкретних соціально-психологічних умовах, а також відсутність ситуацій нанесення психологічної травми особистості та обмеження її прав. Психологічну безпеку також розглядають у вигляді цілісної системи процесів, результатом яких є відповідність потреб, цінностей, можливостей суб'єкта характеристикам реальної дійсності. Різні складові системи можуть виступати як компоненти її розвитку.

Інформаційно-психологічна безпека особистості (ІПБ) – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо. Інформаційно-психологічну безпеку

визначають і як стан захищеності індивідуальної, групової й суспільної свідомості та соціальних суб'єктів різних рівнів від впливу негативних інформаційних факторів, які викликають дисфункціональні соціальні процеси. Таким чином, ІПБ особистості покликана захистити особистість і суспільство від деструктивного інформаційного впливу (рис. 2).

Отже, під **інформаційно-психологічною безпекою** сьогодні прийнято розуміти стан захищеності громадян, їхніх окремих груп і соціальних верств, а також населення в цілому від інформаційно-психологічних впливів, що здійснюються шляхом впровадження деструктивної інформації у свідомість та (або) у підсвідомість людини, що призводить до неадекватного сприйняття ним дійсності.

С. Лихачов розглядає інформаційно-психологічну безпеку як стан захищеності інтересів особистості, суспільства та держави, за якого забезпечується неможливість завдання шкоди духовній сфері людини, культурним надбанням суспільства через використання негативних інформаційно-психологічних впливів [11].

Слід зазначити, що не існує уніфікованих загальноприйнятих визначень вказаного вище ланцюга понять. Проведемо деякі посилання на нормативно-правову базу. В Основному законі України (ст. 17 Конституції) забезпечення інформаційної безпеки України як скла-

дника державної безпеки чітко визначено: забезпечення економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Проте повноваження та функції дер-

жавних органів, а саме в частині забезпечення інформаційно-психологічної безпеки особистості, залишаються неконкретизованими [10].

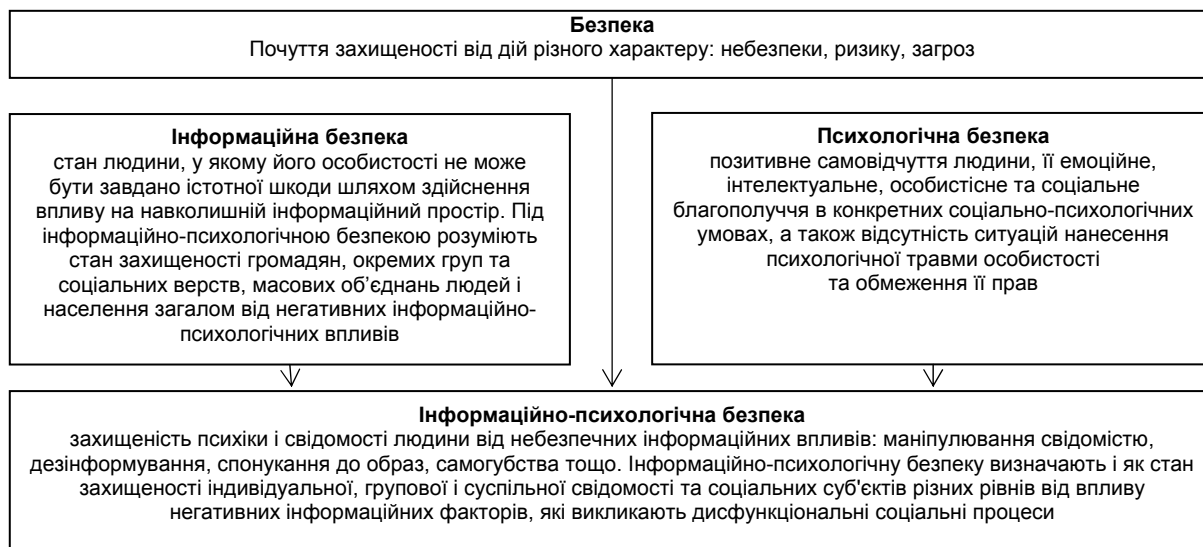


Рис. 2. Інформаційно-психологічна безпека особистості

Закон України "Про національну безпеку України" у ч. 4 ст. 3 формулює, що державна політика у сферах національної безпеки й оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо [8]. Стратегія національної безпеки України [12], а також Стратегія воєнної безпеки України [8], Стратегія інформаційної безпеки [13] визначають актуальні виклики та загрози інформаційній безпеці України в інформаційній сфері, але не наголошують, що одне з головних завдань сучасної держави має бути забезпечення інформаційно-психологічної безпеки особистості, захищеність її психіки та свідомості від негативних інформаційних впливів: маніпулювання, дезінформації.

У Стратегії кібербезпеки України, що є базовим документом у сфері кібербезпеки, взагалі не наводиться понятійно-категорійний апарат [14]. Доктриною інформаційної безпеки України визначено, що національними інтересами України в інформаційній сфері є життєво важливі інтереси особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів. Разом з тим відсутнє визначення поняття інформаційно-психологічна безпека особистості [15].

З метою досягнення цілей та завдань Стратегії національної безпеки України, протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, ефективної протидії пропаганді, деструктивним дезінформаційним впливам та кампаніям, недопущення маніпулювання громадською думкою утворено Центр протидії дезінформації як робочий орган Ради національної безпеки та оборони України [16]. Зокрема, Міністерство оборони України має організовувати і забезпечувати: протидію спеціальним інформаційним операціям, спрямованим

проти ЗСУ та інших військових формувань; супроводження інформаційними засобами виконання завдань оборони України, прогалини законодавчого поля у сфері інформаційної безпеки.

Отже, аналіз наведеної законодавчої бази показав, що основу інформаційно-психологічної безпеки можна розкрити такою, яка перебуває у стані нормативно-правового формування, і тому є потреба в нормативному визначенні поняття "інформаційно-психологічна безпека особистості", яке має бути засноване на відповідних організаційно-психологічних умовах і включати:

- належний рівень теоретичної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів;
- здатність держави створити умови для гармонійного розвитку та задоволення потреб особистості в інформації незалежно від наявності інформаційних загроз;
- забезпечення, розвиток та використання інформаційного середовища на користь особистості;
- захищеність від різноманітних інформаційних загроз.

Сферою активного пізнання в гібридній війні виступає вектор інформаційних впливів на особистість, спрямований на формування деструктивних установок. Це явище отримало назву деструктивний *інформаційно-психологічний вплив* (ІПВ) і трактується як вплив інформації на психіку та свідомість людини, що призводить до неадекватного відображення оточуючої дійсності і як наслідок зміни поведінки [17].

Основними суб'єктами у сфері забезпечення інформаційно-психологічної безпеки особистості є: Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України, міністерства та інші центральні органи виконавчої влади, Національний банк України, ЗСУ, Служба безпеки України, Служба зовнішньої розвідки України, Державна служба спеціального зв'язку та захисту інформації України тощо.

Ураховуючи специфіку діяльності вказаних органів влади, основну мету їхнього створення і чисельність апарату, можна зробити висновок, що вищезазначені органи державного управління можуть ефективно забезпечувати переважно загальнодержавні ідеологічні та захисні заходи від інформаційних загроз суспільству, державі. Поряд із цим забезпечити належний інформаційно-психологічний захист кожної особистості та підвищення, як було зазначено, її власних ресурсів шляхом організаційних, соціальних, психологічних, педагогічних та інших заходів вищевказані суб'єкти інформаційної безпеки фізично не спроможні.

Основними суб'єктами ІПВ є: особи, які приймають рішення, і насамперед військово-політичне керівництво держави; окремі індивіди, військовослужбовці та цивільне населення, у тому числі, дружніх та нейтральних держав; політичні партії; громадські та релігійні організації, меншини; певні соціальні групи (інтелігенція, підприємці, домогосподарки тощо).

Сучасні теорія та практика визначають, що **до основних об'єктів ІПВ належать**: духовний стан особистості; умови та фактори, що забезпечують розвиток усіх сфер життєдіяльності особистості та суспільства; мовне середовище; соціальні, ідеологічні та політичні орієнтири; соціальні зв'язки; психофізичні фактори, що виявляються у вигляді фізичних, хімічних та інших впливів

природного, антропогенного та техногенного походження; генофонд народів, що населяють державу.

Необхідно чітко розуміти, що інформація, яка несе психологічну загрозу, небезпеку, за своєю сутністю не відповідає моральним нормам і є маніпулятивною, часто викликає в людини стан психічної напруги, тривоги, страху, інформаційно-психологічний стрес, психічний розлад та інші психофізіологічні порушення. Тривалий інформаційний вплив, що перевищує допустиму для конкретної людини межу, спонукає інформаційне перенавантаження психіки та призводить до втоми нервових центрів, послідовних реакцій на подразники. Це призводить до послаблення супротиву організму, порушення нормальних фізіологічних функцій, зниження працездатності, виникнення почуття безпорадності та сугестивності. За "успішного" здійснення ІПВ на індивідуальну та суспільну свідомість досягається головне завдання – зміна світоглядних засад суспільства, його духовних цінностей та моральних орієнтирів. Формуються спотворені уявлення та потреби, одночасно нав'язуються чужі ідеали. Відбувається трансформація психологічної безпеки особистості, що може призвести до психічних розладів. Саме тому психологічна безпека особистості та суспільства має займати особливе місце в державній політиці. Структурну схему трансформації психологічної безпеки людини показано на рис. 3.

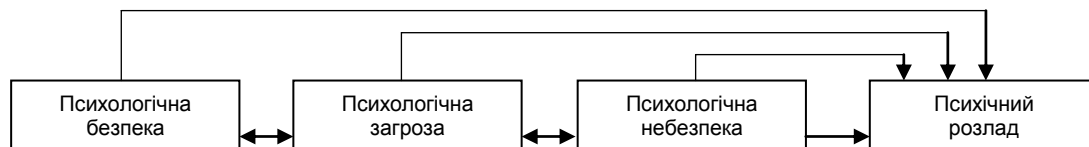


Рис. 3. Структурна схема трансформації психологічної безпеки особистості

Розглядаючи інформаційно-психологічну безпеку особистості як складову інформаційної безпеки, зазначимо, що під **психологічною безпекою** розуміємо позитивне самовідчуття людини, її емоційне, інтелектуальне, особистісне та соціальне благополуччя в конкретних соціально-психологічних умовах, а також відсутність ситуацій нанесення психологічної травми особистості та обмеження її прав. Забезпечення психологічної безпеки – це сукупність дій та заходів суб'єктів безпеки, спрямованих на досягнення стану захищеності життєво важливих інтересів особистості, суспільства і держави.

Таким чином, забезпечення інформаційно-психологічної безпеки особистості має бути виокремлена із загальної сфери інформаційної та психологічної безпеки та буде залежати від вивчення стресових чинників, постстресових розладів, реабілітаційних заходів у разі трансформації психологічної безпеки особистості.

Критеріями ІПБ особистості в суб'єктивному плані виступають її ресурси, рівень захищеності якої від інформаційного впливу залежать від таких внутрішніх факторів:

1) сформованість уявлень про інформаційно-психологічну безпеку (адекватність знань сприяє сві-

домому формуванню захисних механізмів від інформаційних загроз);

2) рівень критичності мислення (здатність піддавати всебічному аналізу різну інформацію з метою з'ясувати ступінь її логічності та ефективності застосування в цій ситуації);

3) ступінь психологічної стійкості (суб'єктивна готовність не піддаватися і не підкорятися інформаційному впливу) [18].

Ураховуючи вищезазначене, можна представити модель інформаційно-психологічної безпеки особистості, де послідовно відображені джерела інформаційних ризиків, особливості інформації, її вплив та задіяння ресурсів особистості. З урахуванням джерел інформаційних ризиків, особливостей інформації та її впливів на особистість, а також компонентів психіки особистості, її ресурсів, можна визначити рівні інформаційно-психологічної безпеки: високий, середній, низький (рис. 4).

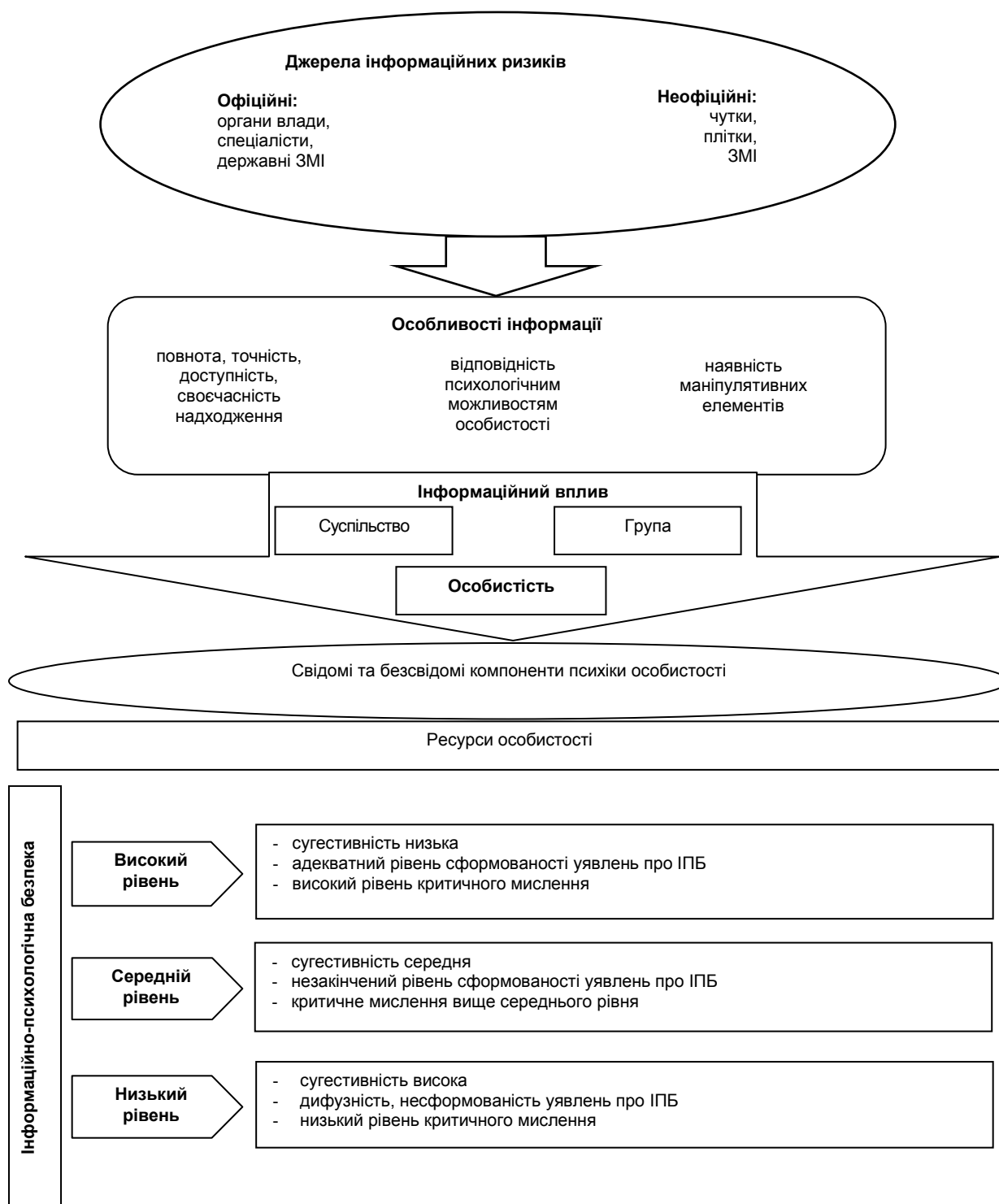


Рис. 4. Модель інформаційно-психологічної безпеки особистості

Поділяючи погляди В. Гусарова, виокремимо такі на-
прямі інформаційно-психологічних атак проти України:

1) широке застосування підконтрольних засобів ма-
сової інформації (у теле-, радіо- та Інтернет-просторі),
ведення за їхньою допомогою пропаганди та створення
необхідного сприятливого інформаційно-психологічного
фону на території України, зокрема з метою здійснення
dezinformacii, нагнітання обстановки, виправдання
агресії, деморалізації патріотично налаштованих кіл
українського суспільства;

2) нав'язування думок про неспроможність українсь-
кої влади керувати державою та приймати раціональні
рішення; формування негативних суджень щодо воєн-
но-політичного керівництва України та про те, що ха-
отичні бойові дії призводять до невиправданих жертв;

3) поширення поглядів про те, що українська армія
на сході України деморалізована та неспроможна ве-
сти бойові дії, а також про недовіру особового складу
до керівництва;

4) нав'язування думки про те, що Україна не обійдеться без російського газу і сторонам необхідно повернутися до перегляду газових контрактів;

5) виключення з радіопростору на підконтрольних РФ територіях загальнодержавних українських теле- й радіоканалів, взяття під контроль регіональних (місцевих) засобів масової інформації тощо;

6) застосування пропагандистських підрозділів в інформаційних та соціальних мережах (на форумах, у соціальних групах, Інтернет-спільнотах) [19].

Розроблення заходів забезпечення інформаційно-психологічної безпеки особистості без їхнього реального втілення та виконання, належного врахування інформаційно-психологічних загроз на рівні держави не призведе до належного захисту особистості, суспільства та держави (табл. 1).

Таблиця 1. Класифікація інформаційно-психологічних загроз

Інформаційно-психологічні загрози				
За наслідками	За методами	За засобами	За об'єктами	За джерелами
В індивідуальній свідомості; у колективній свідомості; у масовій свідомості.	Дезінформація Маніпуляція Пропаганда Шантаж Кризове управління	Державний та спеціальний зв'язок Телерадіомовлення Інтернет, соціальні мережі Друківані ЗМІ Телефон, телеграф, пошта Кіно- і відеопродукція Видавництва і друкарні Бібліотеки й архіви Музеї та експозиції Реклама Виставки тощо	Інтелігенція Службовці, військовослужбовці Підприємці Молодь Пенсіонери Безробітні й ін. соціальні групи	Окремі особи Соціальні групи Суспільство Органи влади держави

На сьогодні питання визначення та класифікації загроз деструктивного ІПВ на індивідуальну та суспільну свідомість є актуальним науковим та прикладним завданням. Особливого значення проблеми інформаційно-психологічної безпеки особистості набувають в умовах виконання обов'язків військової служби. Об'єктом особливого інформаційно-психологічного впливу залишаються свідомість і психіка особового складу ЗС України. Військовослужбовець, будучи повноправним членом суспільства, піддається тим самим деструктивним інформаційно-психологічним впливам як і кожна людина. Проте специфіка виконуваних завдань визначає значущість питань захисту військовослужбовців від ІПВ, оскільки така дія може суттєво підірвати всю систему військової безпеки держави.

Негативними наслідками ІПВ на особовий склад ЗС України в умовах гібридної війни слід вважати:

- розмивання відчуття гордості за свою державу, належності до її збройних сил, підриву переконаності військовослужбовців у необхідності виконувати свій конституційний обов'язок по захисту Українського народу, своєї землі;
- зниження морально-психологічного стану, створення обстановки невпевненості, сумнівів особового складу щодо власного майбутнього, майбутнього збройних сил і держави, послаблення волі до проведення конструктивних реформ, а у воєнний час до збройного опору;
- розкол військових колективів за політичними, релігійними, етнічними, службовими та іншими мотивами, протиставлення солдатського й офіцерського складу;
- погіршення боєздатності частин і підрозділів за рахунок пониження службової активності, дезертирства, симуляції хвороби, ухилення від виконання наказів командирів, зради, колювань і сумнівів у надійності зброї, у придушення волі, створення спотвореної картини бойових дій, бойової обстановки;
- невірне сприйняття військовослужбовцями наявних загроз національній безпеці, дійсних планів і намірів противника.

Ефективними способами протистояння негативному впливу інформаційних потоків є:

моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері;

- розвиток і функціонування системи стратегічних комунікацій сил оборони;
- здійснення правових, організаційних, технічних, інформаційних та інших дій щодо забезпечення власної інформаційно-психологічної безпеки, у тому числі, захисту єдиного інформаційного середовища сил оборони, зокрема в місцях дислокації, розгортання та застосування угруповань, військових частин та підрозділів ЗСУ, інших військових формувань, утворених відповідно до законів України;
- зв'язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в районах здійснення заходів із забезпечення національної безпеки й оборони, відсічі та стримування збройної агресії РФ у Донецькій та Луганській областях;
- протидію інформаційним операціям та іншим заходам інформаційного впливу, спрямованим проти ЗСУ та інших військових формувань, утворених відповідно до законів України;
- донесення достовірної інформації до військовослужбовців ЗСУ, інших складових сил оборони;
- визначення та розробка як один з основних індикаторів (показників) стану національної безпеки такого інтегрованого критерію, як морально-психологічний стан громадян країни (об'єктивно відображає рівень підтримки громадянами державної політики чинної влади), і показників його оцінки (рівень деструктивного зовнішнього та внутрішнього інформаційного впливу);
- підготовки фахівців у сфері інформаційно-психологічного протистояння, розвиток міждисциплінарних наукових і навчальних програм за профілем соціальних комунікацій та інформаційно-психологічної безпеки [13].

Висновки. Набуло подальшого розвитку питання інформаційно-психологічної безпеки особистості в умовах гібридної війни, яке постає як нагальна проблема, і потребує комплексного та системного вирішення. Інфо-

рмаційно-психологічна сфера є ключовим виміром гібридної війни. З огляду на активне використання РФ форм і методів гібридної війни першочерговим завданням стає вироблення ефективної системи захисту особистості від негативних ІПВ, забезпечення інформаційно-психологічної безпеки особистості і суспільства. Основним результатом роботи варто вважати розробку концептуальної моделі інформаційно-психологічної безпеки особистості, яка поєднала у собі існуючі підходи і врахувала напрацювання авторів у попередніх працях. Наголосимо, що одним із першочергових заходів забезпечення інформаційно-психологічної безпеки особистості є розробка та прийняття закону "Про психологічний захист населення" для регулювання негативного впливу на психологічне здоров'я людини.

Перспективи подальших досліджень. Для протидії деструктивним ІПВ гібридній війні в Україні потрібна взаємодія відповідних органів державної та місцевої влади, наукового та експертного середовища. Перспективними необхідно визначити теми та проекти, що виконуються науковими установами:

- з розвитку форм, способів і методики впливу на свідомість (підсвідомість), психічний стан людини;
- подальших розвідок технологій психологічного захисту від негативного ІПВ населення й особового складу ЗС України;
- формування та обґрунтування підходів до вдосконалення системи МПЗ у ЗС України в період наростання воєнної загрози.

Основним результатом діяльності щодо забезпечення інформаційної безпеки особистості має бути збереження здатності військ (сил) і населення до ефективних дій в умовах ІПВ противника.

Список використаної літератури

1. Алещенко В.І. Інформаційно-психологічний вплив у ході збройної боротьби. *Вісн. Київ. Нац. ун-ту імені Тараса Шевченка*, 2018. № 1(38). С. 6–11 [in Ukrainian].
2. Алещенко В.І. Особливості сучасних психологічних операцій Російської Федерації в умовах гібридної війни. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2019. Київ. № 3 [in Ukrainian].
3. Світова гібридна війна: український фронт / За заг. ред. В.П. Горбуліна. Нац. ін-т стратег. досліджень. Київ : НІСД, 2017. 496 с. [in Ukrainian].
4. Кремлівська агресія проти України: роздуми в контексті війни : монографія / Олександр Степанович Власюк, Сергій Володимирович Кононенко, Нац. ін-т стратег. досліджень. Київ : НІСД, 2017. 302 с. [in Ukrainian].
5. Протидія когнітивній війні: інформованість і стійкість. Johns Hopkins University & Imperial College London. NATO Review. URL : <https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kognitivn-vjn-nformovanst-stjks/index.html> (дата звернення: 09.02.2022).
6. Тлумачний словник української мови. У 4 т. / Уклад. : Б. Грінченко. Київ : 1907–1909. Т. 1. С. 43 [in Ukrainian].
7. Стратегія воєнної безпеки України : Указ Президента України від 25 березня 2021 р. № 121/2021. URL : <https://www.president.gov.ua/documents/1212021-37661> (дата звернення: 04.01.2022).
8. Дузь-Крытченко О.П. та ін. Основи стратегії національної безпеки та оборони держави : підруч. – 3-тє вид., перероб. і доп. – К. : НУОУ ім. Івана Черняховського, 2015. 620 с. [in Ukrainian].
9. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 04.01.2022).
10. Конституція України : Закон від 28.06.1996 р. № 254к/96-ВР. URL : <https://www.president.gov.ua/documents/constitution> (дата звернення: 04.01.2022).
11. Лихачов С.В. Інформаційно-психологічна безпека як складова національної безпеки України. *Наук. вісн. 2 (1) '2012. Львів. держ. ун-ту внутрішніх справ*. С. 103–108 [in Ukrainian].
12. Стратегія національної безпеки України. Затв. Указом Президента України від 14 вересня 2020 р. № 392/2020. URL : <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 04.01.2022).
13. Стратегія інформаційної безпеки. Затв. Указом Президента України від 28 грудня 2021 р. № 685/2021. URL : <https://www.president.gov.ua/documents/6852021-41069> (дата звернення: 04.01.2022).

14. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. "Про стратегію кібербезпеки України" : Указ Президента України. URL : <http://zakon.rada.gov.ua/laws/show/96/2016> (дата звернення: 04.01.2022).

15. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 / Президент України. Офіц. вісн. Президента України. 2017. № 5. С. 15 [in Ukrainian].

16. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 р. "Про створення Центру протидії дезінформації" : Указ Президента України від 19 березня 2021 р. № 106/2021. URL : <https://www.president.gov.ua/documents/1062021-37421> (дата звернення: 04.01.2022).

17. Історія інформаційно-психологічного протидіювання : підруч. / Я.М. Жарков та ін. ; за заг. ред. д-ра юрид. наук, проф., засл. юриста України Є.Д. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с. [in Ukrainian].

18. Панченко О.А., Кабанцева А.В. Людська психіка в інформаційній небезпеці. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. Т. 31 (70). № 3. 2020. С. 226–233 [in Ukrainian].

19. Гусаров В. Кремль розпочав нову інформаційну операцію проти України. *Українська правда*. URL : <https://www.pravda.com.ua/news/2014/09/3/7036659/>.

References

1. Aleshchenko VI Information and psychological influence during the armed struggle. Bulletin of the Taras Shevchenko National University of Kyiv, № 1 (38). 2018. P.6–11.
2. Aleshchenko VI Features of modern psychological operations of the Russian Federation in the conditions of hybrid war. "Modern information technologies in the field of security and defense." Kyiv. № 3/2019.
3. World Hybrid War: the Ukrainian front / For the general. ed. VP Gorbunin. National Institute for Strategic Studies. Kyiv: NISS, 2017. 496 p.
4. Kremlin aggression against Ukraine: reflections in the context of war: monograph / A. S. Vlasjuk, S.V. Kononenko, Nat. Inst. of Strategists. research. Kyiv: NISS, 2017. 302 p.
5. Counteracting cognitive warfare: awareness and resilience. Johns Hopkins University & Imperial College London. NATO REVIEW. Website. URL : <https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kognitivn-vjn-nformovanst-stjks/index.html> (access date: 09.02.2022).
6. Explanatory dictionary of the Ukrainian language: in 4 volumes / Compiled by: B. Hrinchenko. Kyiv: 1907-1909. T. 1. Pp. 43.
7. Military Security Strategy of Ukraine. Approved Decree of the President of Ukraine of March 25, 2021 № 121/2021. URL : <https://www.president.gov.ua/documents/1212021-37661> (access date: 04.01.2022).
8. OP Duz-Krytchenko and others. Fundamentals of national security strategy and state defense: textbook. – 3rd ed., Reworked. and ext. – K. : NUOU them. Ivan Chernyakhovsky, 2015. 620 p.
9. "On National Security of Ukraine": Law of Ukraine of June 21, 2018 № 2469-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (access date: 04.01.2022).
10. Constitution of Ukraine: Law of 28.06.1996 №254k / 96-VR. URL : <https://www.president.gov.ua/documents/constitution> (access date: 04.01.2022).
11. Likhachev SV Information and psychological security as a component of national security of Ukraine. Scientific Bulletin 2 (1) '2012. Lviv State University of Internal Affairs. C.103-108.
12. National Security Strategy of Ukraine. Approved Decree of the President of Ukraine of September 14, 2020 № 392/2020. URL : <https://www.president.gov.ua/documents/3922020-35037> (access date: 04.01.2022).
13. Information security strategy. Approved Decree of the President of Ukraine of December 28, 2021 № 685/2021. URL : <https://www.president.gov.ua/documents/6852021-41069> (access date: 04.01.2022).
14. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine": Decree of the President of Ukraine. URL : <http://zakon.rada.gov.ua/laws/show/96/2016> (access date: 04.01.2022).
15. Doctrine of Information Security of Ukraine: Decree of the President of Ukraine of 25.02.2017 № 47/2017 / President of Ukraine. Official Gazette of the President of Ukraine. 2017. № 5. Pp. 15.
16. On the decision of the National Security and Defense Council of Ukraine of March 11, 2021 "On the establishment of the Center for Combating Disinformation": Decree of the President of Ukraine of March 19, 2021 № 106/2021. URL : <https://www.president.gov.ua/documents/1062021-37421> (access date: 04.01.2022).
17. History of information and psychological confrontation: textbook. / YM Zharkov and others; for the head ed. Ph.D., Prof., Assoc. lawyer of Ukraine ED Skulish. Kyiv: Nauk.-ed. Department of the National Security Service of Ukraine, 2012. 212 p.
18. Panchenko OA, Kabantseva AV The human psyche is in informational danger. Scientific notes of TNU named after VI Vernadsky. Series: Public Administration. Volume 31 (70) № 3 2020. pp. 226–233.
19. Gusev V. The Kremlin has launched a new information operation against Ukraine. Ukrainian Pravda. Website. URL : <https://www.pravda.com.ua/news/2014/09/3/7036659/>.

Надійшла до редколегії 04.02.22

V. Aleshchenko, Dr of Psychological Sci., Prof.
avi1953@ukr.net
ORCID ID 0000-0003-1560-7318
Ivan Chernyakhovsky National University of Defense of Ukraine, Kyiv, Ukraine

INFORMATION AND PSYCHOLOGICAL SECURITY OF A PERSON IN THE HYBRID WARFARE CONDITIONS

The article reveals the actualization of the problem of information and psychological security of the individual in a hybrid war. The normative and legal bases of information security as an important component of state security are given. The concepts of security, national security, information security, information-psychological, psychological security are analyzed. The basic criteria of psychological security of the person taking into account information influence are opened. External and internal factors of psychological mechanisms of informational influence on the individual, society, the state as a whole are considered. The main subjects and objects of information and psychological influence are identified. The issue of transformation of psychological security of the individual as a consequence of long-term information and psychological influence is actualized. The structural and functional model of information and psychological security of the individual is given. Theoretical and applied aspects of work with servicemen in the conditions of destructive information influences are summarized and considered. The directions of information and psychological attacks against Ukraine are singled out and the classification of information and psychological threats is given. The negative consequences of information-psychological influence on the psyche are determined and effective ways of counteracting the negative influence of information flows are given. It is emphasized that the control of the information environment, teaching the population the basics of media literacy, taking measures to protect the information environment from external negative influences, etc. contribute to improving the information and psychological security of the individual.

Keywords: information space, information-psychological security, information-psychological influence, moral-psychological state, information-psychological stress.