

УДК 342.9

ВИДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НЕПОВНОЛІТНІХ: НОВИЙ ПОГЛЯД НА УСТАЛЕНІ ПІДХОДИ

Оксана ТОПЧІЙ,
кандидат педагогічних наук

АНОТАЦІЯ

У результаті проведеного аналізу доктринальних джерел з питань інформаційної безпеки автор встановлює, що нате- пер склалася усталена традиція виділяти два основні види: інформаційно-психологічну й інформаційно-технічну. Разом із тим подальший розвиток теорії і виклики практики потребують удосконалення наявних підходів. У статті представлена авторська класифікація видів інформаційної безпеки з наведенням відповідних дефініцій і характерних ознак.

Ключові слова: інформаційна безпека неповнолітніх, види інформаційної безпеки, інформаційно-психологічна безпека, інформаційно-технічна безпека, інформаційно-валеологічна безпека, інформаційно-правова безпека, інформаційно-соціальна безпека.

TYPES OF INFORMATION SAFETY OF MINORS: A NEW LOOK ON ESTABLISHED APPROACHES

Oksana TOPCHII,
Candidate of Pedagogy Sciences

SUMMARY

As a result of the analysis of doctrinal sources on information security, the author states that at present there is an established tradition to distinguish two main types: informational and psychological and informational and technical. However, the further development of the theory and the challenges of the practice require the improvement of existing approaches. The article presents the author's classification of types of information security with the indication of relevant definitions and characteristics.

Key words: information safety of minors, types of information safety, information and psychological safety, information and technical safety, information and valeological safety, information and legal safety, information and social safety.

Загальна постановка проблеми. Інформаційна безпека неповнолітніх (далі – ІБН) останнім часом все більше привертає увагу дослідників. Це пов'язано з низкою причин: інноваційним характером предмета дослідження, подальшим розвитком теорії інформаційної безпеки людини, необхідністю удосконалення правотворчого забезпечення й правозастосовної практики, зрештою, що найголовніше, – прагненням вберегти молоде покоління від небажаних ефектів шкідливого інформаційного впливу. Разом із тим абсолютна більшість учених, розглядаючи цей об'єкт дослідження, не диференціює різновидів його прояву, що у подальшому призводить до певних неточностей і не зовсім релевантних дійсності висновків. У зв'язку з цим виникає потреба творчого розвитку теорії інформаційної безпеки особи, зокрема неповнолітньої.

Виходячи із зазначеного, **мета статті** полягає в обґрунтуванні нових підходів до класифікації видів інформаційної безпеки неповнолітніх. Досягнення поставленої мети можливе за умови розв'язання таких завдань: 1) проаналізувати наявні нате- пер наукові погляди на види ІБН; 2) визначити суттєві складники досліджуваного явища у багатоманітності його проявів; 3) сформулювати авторську інноваційну концепцію класифікації видів ІБН та репрезентувати її для наукового обговорення.

Основні методи дослідження: описовий, формально-догматичний, структурно-функціональний і системного аналізу.

З огляду на інтернаціональний характер проблеми, властивість інформаційних загроз та ризиків негативно впливати на молодь у транснаціональних масштабах, чому великою мірою сприяють процеси глобалізації, автор вважає за потрібне застосування методів порівняльного прогнозування.

Аналіз публікацій. Не зважаючи на те, що в сучасній правовій науці України увага вчених здебільшого зосереджена на розробці шляхів розв'язання проблем інформаційної безпеки держави (і на це є свої занадто поважні причини), питання щодо інформаційної безпеки людини також не залишаються поза колом їхніх інтересів. Чимало в цьому плані зроблено такими науковцями, як: В. Башка-това, Н. Васьковська, О. Дзьобань, О. Довгань, Я. Жарков, О. Золотар, Б. Кормич, В. Ліпкан, А. Лобода, О. Мордань, Н. Новицька, В. Петрик, В. Цимбалюк, М. Швець та ін. Завдяки науковим розвідкам учених нате- пер у правовій науці сформувалися основні методологічні засади розуміння інформаційної безпеки як інституціонального феномена в контексті гносеологічної, онтологічної, аксіологічної парадигми права. Закладені підвалини поняттєво-категоріального апарату теорії інформаційної безпеки. Подальшого творчого розвитку здобули погляди визнаних зарубіжних фахівців у галузі безпекознавства: Н. Віллард, Е. Донахью, Р. Ковальські, С. Лівінгстоун, К. Лідел, С. Лінтон, К. Лідер-мана, Н. Луччі, Б. О'Ніл, Л. Стоун, К. Янг та ін.

Виділення не вирішених раніше частин загальної проблеми. Наукова новизна статті. Незважаючи на застосування окремими вченими вказівок на певні види інформаційної безпеки особистості, знання про ці види ще не набули достатньою мірою систематизованого характеру. Вживання термінології здебільшого базується на узусі, а не на науково обґрунтованій теорії. У зв'язку з цим виникає потреба у репрезентації новітніх підходів до класифікації видів інформаційної безпеки людини, зокрема неповнолітньої особи.

Виклад основного матеріалу дослідження. Багатовимірність полісемічного поняття «інформаційна безпека особи» породжує чимало варіантів його тлумачення.

Характерно, що, даючи визначення, науковці вже апіорі схильються до орієнтації на той чи інший вид безпеки в інформаційній сфері, проте не визначають цього виду. Візьмемо для порівняння принаймні дві дефініції, запропоновані українськими вченими. Наприклад, у трактуванні В. Остроухова і В. Петрика ключове поняття розглядається як «стан захищеності психіки людини від негативного впливу, який здійснюється шляхом упровадження деструктивної інформації у свідомість і (або) у підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності» [1, с. 136] і друга. «Інформаційна безпека особистості – це стан захищеності інтересів особистості підлітка, що характеризується здатністю особистості здійснювати санкціонований доступ до інформаційних ресурсів та забезпечувати безпеку персонального комп'ютера, конфіденційність та цілісність власної інформації, уникати негативних інформаційних впливів і негативних наслідків застосування інформаційних технологій, протизаконних способів збору, поширення й використання інформації та інформаційних технологій» [2, с. 6] Як бачимо, спільним в обох дефініціях є лише виділення одного компонента, через який пояснюється сутність поняття, – «стан захищеності» – і загадка про негативні інформаційні впливи, проте, коли починається конкретизація об'єкта захисту, точки зору кардинально розходяться. Навіть такий простий приклад засвідчує, що йдеться про два принципово різні види інформаційної безпеки. У зв'язку з цим виникає потреба з'ясувати: чи були у доктринальних підходах здійснені спроби класифікації видів інформаційної безпеки людини, зокрема неповнолітньої особи.

Аналіз публікацій засвідчує, що в українській науці стало доволі усталеним розмежування інформаційної безпеки на два види: інформаційно-технічну й інформаційно-психологічну [3–5]. Подібна диференціація базується на логіці розподілу загроз перебігу технічних процесів і загроз психіці і свідомості особистості. Водночас слід зазначити, що питання щодо інформаційно-психологічної безпеки досліджувалося ще задовго до широкого поширення інформаційно-комунікативних технологій [6–10].

Генеза розвитку наукової думки щодо видів інформаційної безпеки, за нашими спостереженнями, на перших етапах характеризувалася відокремленістю гуманітарної та технічної сфери, причому у першій здебільшого були представлені психологи, філософи та соціологи, потім до них долучилися політологи, культурологи й управлінці. У подальшому відбувається інтеграція підходів, й антропологічний складник починає активно розроблятися технічними науками в контексті соціальної інженерії та моделювання суспільних процесів. Особливу увагу вчених привертають питання впливу техногенних факторів на психіку людини, зокрема через уразливість на рівні психофізіологічних та інформаційно-енергетичних впливів, шкоди від застосування психотронної зброї. При цьому зазначається, що здійснення впливу «може бути безпосереднім (у процесі міжособистісного спілкування) і опосередкованим, наприклад, різними технічними засобами» [11, с. 15].

На користь тези, що у сучасній науці відбувається поєднання психологічного та технологічного складників свідчить і той факт, що у новітній монографії «Формування інформаційно-освітнього середовища навчання старшокласників на основі технологій електронних соціальних мереж» окремим параграфом виділяється питання щодо інформаційно-психологічної безпеки, причому остання, за авторською концепцією О. Букова, надається в парі з когнітивною безпекою користувачів комп'ютерної техніки [12, с. 50].

Що ж до правової науки, то вона вирізняється своєю консервативністю й неквапливістю. Ідеї з суміжних наук,

новітні тенденції не дуже швидко переймаються доволі замкненим колом правників. Винятком можуть слугувати трансдисциплінарні дослідження в галузі національної та інформаційної безпеки В. Ліпкана [13–15] й представників його наукової школи та однодумців [16; 17]. Тернистим шляхом палких наукових дискусій прокладаються ідеї, які нині сприймаються як цілком слушні, зокрема щодо питань правового регулювання інформаційної безпеки.

Наприклад, у 2010 р. у рекомендаціях науково-практичної конференції за міжнародною участю «Галузь науки «Державне управління»: історія, теорія, впровадження» Кабінетові Міністрів України пропонувалося розглянути доцільність створення Міністерства інформаційної політики, «яке б несло відповідальність за реалізацію інформаційної політики держави, інформаційно-технічну та інформаційно-психологічну безпеку» [18, с. 472]. Як бачимо, вмсучасних умовах ця ідея реалізована.

Можна констатувати, що наявний нині бінарний розподіл видів інформаційної безпеки на інформаційно-технічну й інформаційно-психологічну, з одного боку, є зручним у застосуванні, з іншого – таким, що у зв'язку із подальшим розвитком науки й викликами практики потребує свого удосконалення в плані подальшої деталізації. Свідченням зрушень є намагання змінити наявні усталені уявлення шляхом запровадження нових категорій. Так, у науковій літературі останніх років можна зустріти терміни-неологізми: інформаційно-культурна безпека [19], комунікаційно-контентна безпека [20] та ін.

Було б неправильним вважати, що до цього часу не робилися спроби винайти найбільш точні тлумачення ключових термінів і розширити діапазон видів інформаційної безпеки. Наприклад, С. Барінов пропонує розуміти під інформаційною безпекою особистості «стан захищеності, за якого відсутній ризик, пов'язаний із заподіянням інформаційної шкоди здоров'ю і (або) фізичному, психічному, духовному, моральному розвитку людини» й шляхом огляду наукових праць інших учених, цитації їх тлумачень обґрунтовує ідею виділення, окрім уже наявних та усталених категорій (інформаційно-технічна, інформаційно-психологічна безпека) ще й інформаційно-ідеологічну та інформаційно-правову безпеку [21, с. 102–103]. У деталізації понять учений характеризує зазначені види безпеки таким чином:

– *інформаційно-технічна* – «захищеність інформації та інфраструктури, що підтримується, від випадкових або навмисних впливів природного чи штучного характеру, що загрожує нанесенням шкоди володільцям або користувачам інформації або підтримуючої інфраструктури» [21, с. 102]. Принагідно зауважимо, що за такого підходу взагалі скоріше йдеться про безпеку інформації, а не інформаційну безпеку особистості. Зокрема, не згадуються техногенні чинники впливу на особистість, психотронна зброя тощо. По суті, подібна інтерпретація може кваліфікуватися здебільшого в контексті класичного інформаційного або цивільного права;

– *інформаційно-ідеологічна* – «захищеність особистості від навмисного або ненавмисного інформаційного впливу, що має результатом порушення прав і свобод у галузі створення, користування і поширення інформації, користування інформаційною структурою і ресурсами, які протирічать моральним та етичним нормам, здійснюють деструктивний вплив на особистість, який має негласний (позачуттєвий, неусвідомлений) характер і впроваджує в громадську свідомість антисоціальні установки». [21, с. 102–103]. Подібне тлумачення взагалі не можна вважати релевантним семантиці терміна з низки причин. По-перше, тут представлені загальні права і свободи людини, що існують, насамперед як правові, а не ідеологічні інституції, а зна-

чить, їх варто було б розглядати в категорії інформаційно-правової безпеки. По-друге, в одному ряду із загально-визнаними, конституційно закріпленими правами людини наводяться делікти, які за своєю сутністю не можна трактувати як ідеологеми. По-третє, тут взагалі відсутні будь-які натяки на певну ідеологію, адже традиційно ця тема розглядається на дихотомічній осі «особистість – держава». Поняття антисоціальних установок домінує насамперед на рівні суспільства, що може бути противагою лише пріоритетам, які представлені в парадигмі чітко артикульованої державної політики, інакше втрачається сенс згадувати про них;

– *інформаційно-психологічна* – «стан захищеності психіки особистості від впливу багатоманітних інформаційних чинників, які перешкоджають або ускладнюють формування й функціонування адекватної інформаційно-орієнтувальної основи соціальної поведінки людини (і в цілому життєдіяльності у суспільстві), а також адекватної системи її суб'єктивного (особистісного, суб'єктивно-особистісного) ставлення до оточуючого світу і самої себе» [21, с. 103]. Позитивною стороною цього визначення, на наш погляд, є вказівки на багатфакторність впливу, на об'єкт загроз, на взаємозв'язок людини і соціуму. Проте за межами дефініції залишилися такі важливі процеси, як психологічні засади формування й трансформації під впливом інформаційних чинників свідомості, зокрема правової, підтримка ментального здоров'я особистості тощо;

– *інформаційно-правова* – «стан захищеності права людини шукати, отримувати, передавати, виробляти й поширювати інформацію, а також права на недоторканість інформації щодо особистого життя» [21, с. 103]. У наведеному контексті йдеться не про правовий захист самої людини, що є стрижневим компонентом антропоцентричної моделі, а про захист доволі звужених інформаційних прав. У такий спосіб прочитована дефініція не може задовольнити всім вимогам щодо розуміння семантики термінологічного словосполучення.

Таким чином, поцінуючи спробу автора розширити уявлення про види інформаційної безпеки завдяки введенню до наукового обігу додаткових категорій, ми вважаємо, що і самі запропоновані до розгляду компоненти, і їх тлумачення є скоріше дискусійними, аніж загально-прийнятими.

З огляду на нагальність питання дослідження інформаційної безпеки неповнолітніх із поступовим втіленням його основних засад у державну інформаційну політику, нормативно-правові акти, практику правозастосування, ми пропонуємо власну концепцію класифікації видів ІБН, яка являє собою творчий розвиток наявних усталених підходів. Одразу оговоримо так: 1) ми чітко усвідомлюємо умовність розподілу компонентів в межах класифікації (і з позицій їх виділення, і з позицій їх репрезентації); 2) диференціація компонентів не ліквідує їхні взаємозв'язки і взаємовплив, а є лише намаганням окреслити ті явища, які мають своєрідні характеристики, а звідси – потребують свого інструментарію під час вирішення проблеми забезпечення безпеки.

Отже, за нашими уявленнями, видами інформаційної безпеки особи, зокрема неповнолітньої, слід виділяти: інформаційно-психологічну, інформаційно-валеологічну, інформаційно-соціальну, інформаційно-правову та інформаційно-технічну безпеку. Охарактеризуємо кожен із зазначених видів.

Інформаційно-психологічна безпека неповнолітнього – сегмент національної/інформаційної безпеки людини, суспільства і держави, що являє собою стан, процес і результат цілеспрямованої діяльності держави, інститутів громадянського суспільства, всіх свідомих суб'єктів

інформаційних правовідносин щодо захисту психіки й свідомості особи від деструктивних впливів, створення умов для повноцінного гармонійного розвитку та самореалізації особистості.

Зазначені у визначенні деструктивні впливи спрямовані насамперед на зміну психологічних станів (наприклад, спонукання до агресії, психологічного насильства, введення у депресію тощо), появу фобій та необґрунтованої постійної тривоги, демотивацію діяльності, неадекватність самооцінки (заниження або перевищення), формування залежностей (адикції) – ігрової, хімічної та ін.

Особливо небезпечною для неповнолітніх категорію становлять технології, що ведуть до стійких психічних розладів.

Головним інструментарієм забезпечення інформаційно-психологічної безпеки неповнолітнього виступає експертна, консультативна, просвітницька, корекційна діяльність психологів і педагогів, їхні рекомендації уповноваженим органам влади щодо нормативного врегулювання процесів поширення небажаної для суспільства інформації.

Інформаційно-валеологічна безпека неповнолітнього (від лат. *valere* – бути здоровим + *logos* – наука, вчення) [22, с. 111] – вид інформаційної безпеки, спрямований на захист особи від негативного впливу інформації, яка може призвести до суїциду або особливо небезпечних травм чи хвороб, погіршення стану здоров'я через куріння, вживання алкогольних, наркотичних та ін. шкідливих речовин, нерозбірливих статевих відносин, навмисного пошкодження частин тіла чи шкіри (зокрема, через шрамінг або татування), потягу до нездорової їжі (фастфуду) чи біодобавок із одночасним протиставленням цьому здорового способу життя, культури тіла й фізичної активності.

У формуванні дефініції ми спираємося на визначення валеології, надане в «Енциклопедії освіти»: «Валеологія – наука про закономірності й механізми формування, збереження, зміцнення, відновлення та передачі за спадковістю здоров'я» [23, с. 72]. Принагідно слід зазначити, що, за спостереженнями В. Грибана, запровадження валеології як навчальної дисципліни в закладах освіти України датується 1994 роком [24, с. 8].

Відокремлення інформаційно-валеологічної безпеки від інформаційно-психологічної, незважаючи на їх тісний взаємозв'язок і детермінацію поведінки психічною діяльністю людини, ми пояснюємо намаганням диференціювати вітальні процеси, спрямовані на збереження життя і фізичного здоров'я, і суто психологічні процеси. Можна констатувати, що інформаційно-валеологічна безпека виростає з психологічного підґрунтя і переходить у сферу практичної (профілактичної) медицини, прагмапедагогіки, права та ін. наук.

На користь виділення інформаційно-валеологічної безпеки як окремого виду з позицій права свідчать такі аргументи:

– закріплення у ст. 3 Конституції України положення, що «людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю» [25];

– наявність у преамбулі Основ законодавства України про охорону здоров'я тези про те, що «суспільство і держава відповідальні перед сучасним і майбутніми поколіннями за рівень здоров'я і збереження генофонду народу України, забезпечують пріоритетність охорони здоров'я в діяльності держави, поліпшення умов праці, навчання, побуту і відпочинку населення, розв'язання екологічних проблем, вдосконалення медичної допомоги і запровадження здорового способу життя» [26];

– наведення у переліку засад державної політики у сфері освіти та принципів освітньої діяльності в ст. 6 Закону

Україні «Про освіту» позиції щодо «формування культури здорового способу життя» [27];

– виділення у Кримінальному кодексі України окремого розділу II – «Злочини проти життя та здоров'я особи» [28];

– схвалення постановою Верховної Ради України Рекомендацій парламентських слухань про становище молоді в Україні «Формування здорового способу життя української молоді: стан, проблеми та перспективи» [29];

– розрізнення фізичного, сексуального, психологічного, економічного насильства в Концепції державної соціальної програми запобігання та протидії домашньому насильству та насильству за ознакою статі на період до 2023 р., схваленою розпорядженням Кабінету Міністрів України від 10 жовтня 2018 р. № 728 р. [30].

У запропонованому нами новому виді інформаційної безпеки варто виділяти два види загроз: 1) за квантитативними (кількісними) ознаками – шкідливий вплив на здоров'я особи тривалого користування комп'ютером, мобільних пристроїв, засобів відтворення аудіопродукції, що призводить до гіподинамії, остеопатії, проявів зап'ястного синдрому, зниження показників слуху і зору, ефекту «сухого ока», запаморочень, порогових знижень концентрації уваги тощо; 2) за квалітативними (якісними) ознаками – негативний вплив контенту інформаційних ресурсів на поведінку неповнолітніх й організацію ними свого дозвілля у небезпечний спосіб: активізація ризикованої поведінки, поява осередків так званих «зачеперів» (поїздка на непристосованих для цього місцях транспортних засобів), «паркурістів» (переміщення небезпечними поверхнями і екстремальне подолання перешкод), «фрістайлерів» («акробатичні етюди» у стрибках і вільному падінні) «джампінгістів» (стрибки з висоти за відсутності страховальних засобів), «маунтбейкерів» (їзда на велосипеді з крутих схилів, не пристосованих для пересування) тощо. Сюди ж ми відносимо такі традиційно негативні звички, що шкодять здоров'ю людини, а й іноді ставлять під загрозу її життя, як потяг до алкоголю, куріння (зокрема, електронних сигарет і кальянів), вживання наркотичних, медикаментозних (не за призначенням) препаратів і хімічних речовин та ін. Окреме місце у цій категорії займають питання збереження сексуального й репродуктивного здоров'я молоді.

Головним інструментарієм забезпечення інформаційно-валеологічної безпеки неповнолітнього виступає праворегулювальна й правозастосовна діяльність, зокрема в частині нормування змісту кіно-, теле- і медіа-продукції, реклами; просвітницька й дозвільна робота шкільних і позашкільних закладів освіти; діяльність органів місцевого самоврядування щодо екологічного стану довкілля, впорядкування територій, організації спортивних майданчиків, своєчасна реакція на появу так званих «наркографіті» з інформацією щодо джерел придбання шкідливих для здоров'я речовин; сімейне виховання. Як бачимо, навіть на рівні інструментарію є суттєві відмінності у забезпеченні інформаційно-психологічної та інформаційно-валеологічної безпеки, що слугує ще одним підтвердженням необхідності диференціації зазначених понять.

Інформаційно-правова безпека неповнолітнього – невіддільна частина інформаційної безпеки людини, спрямована на застосування правових механізмів для захисту інформаційних прав і свобод людини, убезпечення дитини від непризначеної для неї інформації та упередження інформаційних деліктів. Специфіка цього виду безпеки з позицій права полягає у поєднанні забезпечувальних та оборонних чи обмежувальних засобів. Наприклад, поряд із забезпеченням права неповнолітнього на доступ до інформації вступає в дію обмеження такого доступу або через наявність таємниці (державної, банківської,

медичної, таємниці усиновлення чи таємниці штучного запліднення від донора), або через наявність небажаного для такого віку особи контенту. Зазначений вид безпеки тісно пов'язаний із такими юридичними категоріями, як «правова культура», «правове виховання», «правова просвіта», «правова свідомість», «безпечне інформаційне середовище» тощо. Завдяки комплексному використанню правового та освітньо-виховного інструментарію можлива превенція інформаційних деліктів, що вчинюються неповнолітніми.

Інформаційно-соціальна безпека неповнолітнього – сегмент національної/інформаційної безпеки людини, суспільства і держави, за якого правовими, організаційно-управлінськими та ін. засобами створюються умови для повноцінного розвитку особистості як достойного законслухняного члена спільноти з активною громадянською позицією й убезпечення неповнолітньої особи від негативних інформаційних впливів деструктивних спільнот (кримінальних, екстремістських, релігійних та ін.).

Виділення цього виду ІБН зумовлене тим, що особа виступає не лише як індивід, а і як член певного мікро- і макросоціуму. Залежно від оточення, в якому перебуває особистість, – сімейного, шкільного, позашкільного, віртуального, медійного – формується й закріплюється її система поглядів, переконань, ціннісні орієнтири, які у подальшому скеровують поведінку неповнолітнього, що не може не відобразитися на безпеці суспільства в цілому.

Інструментарієм забезпечення інформаційно-соціальної безпеки виступає правове регулювання інформаційних правовідносин, важелі державної інформаційної політики, соціально-етичні норми, освітньо-виховні засоби тощо.

Інформаційно-технічна безпека неповнолітнього – складник інформаційної безпеки особистості, що передбачає поєднання інформаційно-технологічних компетенцій із застосуванням заходів технічної безпеки, формуванням відповідального ставлення до роботи з інформацією, ресурсами, пристроями, до процедур збирання, зберігання, поширення інформації.

Такий вид інформаційної безпеки як жодний інший взаємопов'язаний із функціонуванням кібербезпеки, оскільки він, на відміну від усіх інших, не може реалізовуватися у безпосередньому спілкуванні без застосування відповідних технічних засобів.

Інструментарієм забезпечення інформаційно-технічної безпеки є насамперед комплекс технічних заходів, використання спеціального програмного забезпечення, зокрема систем батьківського контролю, у поєднанні із освітньо-виховною діяльністю.

Таким чином, запропонована нами класифікація видів інформаційної безпеки неповнолітнього досить повно охоплює всі аспекти забезпечення, дає змогу в кожному окремому напрямі встановити дієві механізми регулювання правовідносин.

Висновки. Під час проведеного дослідження вдалося встановити, що в сучасній правовій науці України усталеності набула концепція, за якої умовний розподіл видів інформаційної безпеки здійснюється за двома категоріями: інформаційно-психологічна й інформаційно-технічна. Аналіз публікацій останніх років виявив, що, по-перше, відстежується тенденція взаємопроникнення двох зазначених напрямів, а по-друге, відбувається намагання вчених розширити діапазон уявлень про наявні види безпеки, що є доволі симптоматичним. У зв'язку з цим удалося сформулювати та репрезентувати оригінальну авторську класифікацію, що у подальшому відкриває широкі перспективи як для наукових досліджень, так і для удосконалення практичної діяльності.

Список використаної літератури:

1. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. Політичний менеджмент. 2008. № 4. С. 135–141.
2. Ковальчук В.Н. Забезпечення інформаційної безпеки старшокласників у комп'ютерно-орієнтованому навчальному середовищі: автореф. дис. ... канд. пед. наук: 13.00.10; Ін-т інформ. технологій і засобів навчання НАПН України. К., 2011. 20 с.
3. Гавришак Л. Інформаційно-психологічна безпека особистості у сучасному світі. Проблеми гуманітарних наук. Серія: Психологія. 2012. Вип. 29. С. 100–110. URL: http://nbuv.gov.ua/UJRN/Pgn_ps_2012_29_9.
4. Остроухов В.В. Інформаційно-психологічна безпека особи. URL: <http://westudents.com.ua/glavy/51809-11-nformatsyno-psihologichna-bezpeka-osobi.html>.
5. Мануйлов С.М., Калиновський Ю.Ю. Роль і місце інформаційної безпеки у розбудові сучасної української держави. Вісник нац. ун-ту «Юридична академія України імені Ярослава Мудрого». 2016. № 2 (29). С. 144–153.
6. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М.: Изд-во РАГС, 1998. 125 с.
7. Грачев Г.В., Мельник И.К. Манипулирование личностью: организация, способы и технологии информационно-технологического воздействия. М.: Алгоритм, 2002. 288 с.
8. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). Мн.: Харвест, 1999. 448 с.
9. Проблемы информационно-психологической безопасности / под ред. А.В. Брушлинского и В.Е. Лепского. М.: Ин-т психологии РАН, 1996. 100 с.
10. Рошин С.К., Соснин В.А. Психологическая безопасность: новый подход к безопасности человека, общества и государства. Российский монитор. 1995. № 6. URL: <http://www.bookap.by.ru/psywar/grachev/gl6.shtml>
11. Мохор В., Цуркан О. Негативний інформаційно-психологічний вплив на індивідуальну свідомість за соціоінженерним підходом. Information Technology and Safety. July–December 2017. Vol. 5. Iss. 2 (9). С. 13–18. URL: http://ela.kpi.ua/bitstream/123456789/23928/1/ITS2017.5.2%289%29_02.pdf.
12. Буров О.Ю. Інформаційно-психологічна та когнітивна безпека користувачів ЕСМ. Формування інформаційно-освітнього середовища навчання старшокласників на основі технологій електронних соціальних мереж: монографія / В.Ю. Биков, О.П. Пінчук, С.Г. Литвинова та ін.; наук. ред. О.П. Пінчук. К. Педагогічна думка, 2018. 160 с. С. 50–53.
13. Ліпкан В.А. Адміністративно-правове регулювання національної безпеки України: монографія. К.: Текст, 2008. 440 с.
14. Ліпкан В.А. Безпекознавство: навчальний посібник. К.: Вид-во Європ. ун-та, 2003. 208 с.
15. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України: монографія. К.: Текст, 2003. 600 с.
16. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с. (Серія: Національна і міжнародна безпека).
17. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України: Глосарій. К.: Текст, 2004. 136 с.
18. Рекомендації науково-практичної конференції за міжнародною участю «Галузь науки «Державне управління»: історія, теорія, впровадження» (Київ, 28 травня 2010 р.). Наукове видання. Матеріали науково-практичної конференції. Т. 2. К.: Нац. акад. держ. упр. при Президентові України, 2010. С. 472–474.
19. Мануйлов С.М., Прудникова О.В. Інформаційно-культурна безпека України в умовах «гібридної війни». Вісник нац. ун-ту «Юридична академія України імені Ярослава Мудрого». 2017. № 1 (32). С. 26–36.
20. Любовець Г., Король В. Комунікативно-контентна безпека як глобальний напрям розвитку креативних індустрій у безпековій сфері. Мова і суспільство. 2017. Вип. 8. С. 47–55.
21. Баринов С.В. О правовом определении понятия «информационная безопасность личности». Актуальные проблемы российского права. 2016. № 4 (65). С. 97–105.
22. Новий словник іншомовних слів: близько 40 000 слів і словосполучень / Л.І. Шевченко, О.І. Ніка, О.І. Хом'як, А.А. Дем'янюк; За ред. Л.І. Шевченко. К.: Арії, 2008. 672 с.
23. Енциклопедія освіти / Акад. пед. наук України; головний ред. В.Г. Кремень. К.: Юрінком Інтер, 2008. 1080 с.
24. Грибан В.Г. Валеологія: підручник. К.: Центр учбової літератури. 2008. 214 с.
25. Конституція України від 28.06.96 р. № 254/96 ВР. Відомості Верховної Ради (ВВР) України. 1996. № 30. Ст. 141.
26. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 № 2802-ХІІ. Відомості Верховної Ради України, 1993, № 4, ст. 19.
27. Про освіту: Закон України від 05.09.2017 р. № 2145-19. ВВР України. 2017. № 38–39. Ст. 380.
28. Кримінальний кодекс України від 05.04.2001 № 2341-ІІІ. Відомості Верховної Ради України, 2001, № 25–26, ст. 131.
29. Про рекомендації парламентських слухань про становище молоді в Україні «Формування здорового способу життя української молоді: стан, проблеми та перспективи»: Постанова Верховної Ради України від 03.02.2004. Відомості Верховної Ради України, 2004, № 16, ст. 243.
30. Концепція державної соціальної програми запобігання та протидії домашньому насильству та насильству за ознакою статі на період до 2023 р., схвалена розпорядженням Кабінету Міністрів України від 10 жовтня 2018 р. № 728-р. Урядовий кур'єр від 03.11.2018, № 207.

ІНФОРМАЦІЯ ПРО АВТОРА

Топчій Оксана Василівна – кандидат педагогічних наук

INFORMATION ABOUT THE AUTHOR

Topchii Oksana Vasylivna – Candidate of Pedagogy Sciences