DOI https://doi.org/10.51647/kelm.2020.3.2.37

ОКРЕМІ АСПЕКТИ СОЦІАЛЬНОГО ЧИННИКА В ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ СУСПІЛЬСТВА

Анатолій Тарасюк
кандидат юридичних наук,
головний науковий співробітник наукової лабораторії забезпечення
інформаційної та кібернетичної безпеки
Науково-дослідного інституту інформатики і права Національної академії правових наук України
(Київ, Україна)
ORCID ID: 0000-0002-0479-0666

Анотація. У праці визначаються місце в системі наукового знання загальної теорії інформаційної безпеки, яка консолідує всі частини інформаційно-пізнавального цілого в системі інформаційної та кібернетичної безпеки, а також специфіка її розвитку й головні завдання. Надзвичайна вагомість захисту суспільства від інформаційно-кібернетичних викликів і загроз зумовлює потребу формування загальної теорії інформаційної безпеки, передовсім її соціально-філософських засад. Водночас розглянуті у статті соціальні інформаційно-безпекові заходи стануть запорукою поширення й затвердження в суспільстві в межах новостворюваної загальнонаукової теорії інформаційної та кібернетичної безпеки, відповідної соціально-філософської концепції.

З'ясовано особливості загальної теорії кібернетичної безпеки, яка перебуває на етапі свого формування. Визначено місце в системі наукового знання та основні завдання цієї теорії, покликаної інтегрувати в інформаційно-безпековій системі всі інформаційно-когнітивні складники. Особлива вагомість і значущість захисту від викликів і загроз в інформаційній сфері зумовлюють нагальну потребу закладення соціально-філософських підвалин загальної теорії інформаційної та кібернетичної безпеки. Водночас соціальні інформаційно-безпекові заходи сприятимуть популяризації та впровадженню в суспільну свідомість соціально-філософської концепції інформаційної та кібербезпеки. Вказані засади, на нашу думку, конкретизуватимуть зазначену теорію, дадуть поштовх її розвиткові, торуючи гуманістичний напрям. А це, зі свого боку, зумовить відповідні трансформації суспільної свідомості щодо усвідомлення сутності інформаційної та кібербезпеки, її особливостей та значення.

Ключові слова: кібербезпека, права особи, інформаційна безпека, інформаційне суспільство.

CERTAIN ASPECTS OF THE SOCIAL FACTOR IN PROVIDING CYBER SECURITY OF SOCIETY

Anatoliy Tarasyuk
Candidate of Law,
Chief Researcher at the Scientific Laboratory for Information and Cyber Security
Research Institute of Informatics and Law of the National Academy of Pedagogical Sciences of Ukraine
(Kyiv, Ukraine)
ORCID ID: 0000-0002-0479-0666

Abstract. This paper defines the place in the system of scientific knowledge of the general theory of information security, which consolidates all parts of the information-cognitive whole in the system of information and cyber security, as well as the specifics of its development and main tasks. The extraordinary importance of protecting society from information and cybernetic challenges and threats necessitates the formation of a general theory of information security, especially its socio-philosophical foundations. At the same time, the social information and security measures considered in the article will become a guarantee of dissemination and approval in society, within the framework of the newly created general scientific theory of information and cyber security, the corresponding socio-philosophical concept.

The peculiarities of the general theory of cyber security, which is at the stage of its formation, are clarified. The place in the system of scientific knowledge and the main tasks of this theory, designed to integrate all information and cognitive components in the information and security system, are determined. The special importance and significance of protection against challenges and threats in the information sphere determine the urgent need to lay the socio-philosophical foundations of the general theory of information and cyber security. At the same time, social information and security measures will promote and popularize the social and philosophical concept of information and cybersecurity in the public consciousness. These principles, in our opinion, will concretize this theory, give impetus to its development, paving the humanistic direction. And this, in turn, will lead to appropriate transformations of public consciousness to understand the essence of information and cybersecurity, its features and significance.

Key words: cybersecurity, individual rights, information security, information society.

WYBRANE ASPEKTY CZYNNIKA SPOŁECZNEGO W ZAPEWNIENIU CYBERBEZPIECZEŃSTWA SPOŁECZEŃSTWA

Anatolii Tarasiuk
kandydat nauk prawnych,
główny pracownik naukowy Laboratorium Naukowego Bezpieczeństwa Informacji i Cyberbezpieczeństwa Naukowo-Badawczego Instytutu Informatyki i Prawa Narodowej Akademii Nauk Prawnych Ukrainy
(Kijów, Ukraina)
ORCID ID: 0000-0002-0479-0666

Adnotacja. Praca ta określa miejsce w systemie wiedzy naukowej ogólnej teorii bezpieczeństwa informacji, konsolidującej wszystkie części całości informacyjno-poznawczej w systemie bezpieczeństwa informacji i cybernetycznego, a także specyfikę jego rozwoju i główne zadania. Ekstremalna waga ochrony społeczeństwa przed wyzwaniami i zagrożeniami informacyjno-cybernetycznymi warunkuje potrzebę stworzenia ogólnej teorii bezpieczeństwa informacji, przede wszystkim jej podstaw społeczno-filozoficznych. Jednocześnie omówione w artykule społeczne środki bezpieczeństwa informacji staną się kluczem do rozpowszechniania i zatwierdzania w społeczeństwie, w ramach nowo utworzonej ogólnej naukowej teorii bezpieczeństwa informacji i cyberbezpieczeństwa, odpowiadającej koncepcji społeczno-filozoficznej.

Wyjaśniono cechy ogólnej teorii bezpieczeństwa cybernetycznego, która jest na etapie powstawania. Określono miejsce w systemie wiedzy naukowej i główne zadania tej teorii, mające na celu zintegrowanie w systemie informacyjnego bezpieczeństwa wszystkich składników informacyjno-poznawczych. Szczególna ważność i znaczenie ochrony przed wyzwaniami i zagrożeniami w dziedzinie informacji przesądza o potrzebie tworzenia społeczno-filozoficznych podstaw ogólnej teorii bezpieczeństwa informacji i cyberbezpieczeństwa. W tym samym czasie, środki bezpieczeństwa informacji społecznej przyczyni się do popularyzacji i wdrażania do świadomości społecznej koncepcji społeczno-filozoficznej informacji i cyberbezpieczeństwa. Wspomniane zasady, naszym zdaniem, będą konkretyzować wspomnianą teorię, dadzą impuls do jej rozwoju, wpływając na kierunek humanistyczny. A to z kolei warunkuje odpowiednie przemiany świadomości społecznej w odniesieniu do świadomości istoty informacji i bezpieczeństwa cybernetycznego, jej cech i znaczenia.

Słowa kluczowe: cyberbezpieczeństwo, prawa osób fizycznych, bezpieczeństwo informacji, społeczeństwo informacyjne.

Вступ. Як доведено всією історією людства, безпека є атрибутом його нормального існування. Водночас постійно зростає гуманістична спрямованість процесу її забезпечення. У контексті сьогодення це дасть змогу створити безпечні умови використання суспільством інформаційних технологій та кіберпростору, запобігаючи та знешкоджуючи виклики та загрози інформаційного характеру.

Успішне створення умов безпечного функціонування в кібернетичному просторі потребує значних зусиль і ретельної попередньої підготовки. Аналіз можливостей новітніх технологій та їх майбутніх потенцій доводить, що вкрай важливо, щоб новітні цифрові технології не втратили соціальний зміст і не набули антигуманістичної спрямованості. Варто також наголосити, що вектор нових інформаційних технологій визначається не стільки їх розробниками, скільки самим суспільством, де формується відповідне соціальне середовище – гуманістичне чи з префіксом анти-.

Основна частина. *Матеріалами дослідження* першочергово стали міжнародні стандарти, норми міжнародного та національного права, аналіз діяльності міжнародних компаній. Використано загальнотеоретичні (*гносеологічний, функціонально-структурний*) та спеціальні (*порівняльно-правовий, індуктивний*) методи дослідження.

Результати та їх обговорення. Для розвитку людської цивілізації, її виживання неабиякої вагомості набуває оцінка технічних «інфо-кібер-технологічних» новацій та прогноз щодо їх використання. Зрозуміло, що володіння достеменною інформацією стосовно можливих напрямів застосування комп'ютерних технологій істотно сприяє убезпеченню від можливих різноманітних шкідливих наслідків. Натомість «гарантом» майбутніх негараздів (аварій, катастроф тощо) є нерозуміння наслідків застосування вказаних технологій, отримання неповної, недостовірної, спотвореної чи хибної інформації. Водночас, як зазначають фахівці з кібербезпеки, «кіберзагрози еволюціонують в прискореному темпі, вони стають досконалішими, краще організованими і транснаціональними» (Трофименко, 2019: 101). Тобто головним дороговказом на шляху розвитку системи інформаційних технологій має стати прийдешнє людства. Тому, на наше глибоке переконання, структура глобальної світової безпекової системи обов'язково зазнає позитивних змін з огляду на зміщення в гуманістичний бік пріоритетів у змісті кібернетичної безпеки.

Тож забезпечення якнайширшого різноманіття в інформаційних мережах правомірного контенту в контексті захисту основних людських прав і свобод і громадянина – це задоволення передовсім саме тих інформаційних потреб, які відповідають інтересам прогресу світової цивілізації. Тобто, коли йдеться про інформаційно-телекомунікаційні технології, які спрямовані на повагу до загальнолюдських цінностей, якраз і передбачається, що виключно на прогресивний поступ спрямовуватиметься оволодіння соціумом знанням та інформацією за допомогою технологій.

Забезпечення ж загального рівного доступу до інформації та відповідних технологій передбачає насамперед розширення соціальної бази кібернетичної безпеки, що посприяє оптимізації всіх рівнів функціонування – особистісного, суспільного й державного. У цьому, звісно, зацікавлене громадянське суспільство, котре проголошує

рівні можливості, в тому числі й стосовно участі в інформаційних комунікаціях, для усіх своїх членів. Таке розширення соціальної бази інформаційної безпеки означає водночас ріст кількості її суб'єктів. Тож виникає важливе завдання підвищення рівня інформаційної культури, освіченості вказаних соціальних суб'єктів й суспільства загалом. Це рівною мірою стосується і професійної діяльності в галузі інформаційно-телекомунікаційних технологій, і взагалі будь-якої діяльності в інформаційній сфері, котра охоплює всіх суб'єктів інформаційних відносин при використанні кіберпростору. Позаяк безпеку соціуму визначає, врешті-решт, саме рівень головної передумови формування соціально-економічного, наукового, культурного й духовного потенціалу – людського ресурсу. Тому, зважаючи на наведені резони, визначальними чинниками забезпечення надважливого складника національної безпеки – інформаційної та кібернетичної безпеки – вбачаються наука й освіта.

Зростання в інформаційній безпеці ролі соціального складника зумовлює, на нашу думку, потребу запровадження принципово нового виду захисних інформаційно-безпекових заходів – соціальних. Якісною новизною вказаний вид захисту інформаційної безпеки особи, суспільства й держави зобов'язаний складній, багаторівневій системі механізмів і поведінкових форм, сукупність котрих і мусить цю безпеку забезпечити.

Задля успішного розв'язання проблем забезпечення кібернетичної безпеки потрібне, на нашу думку, впровадження комплексу заходів, а саме:

– проведення активного наукового пошуку в межах розвитку інформаційної етики – нової галузі етичного знання, котра перебуває на етапі свого становлення;

– освітні та виховні заходи;

– всебічна популяризація в суспільній свідомості способів, моделей і форм морально-етичної поведінки у глобальному кіберсередовищі із застосуванням при цьому найсучасніших цифрових технологій, із залученням усіх можливих ЗМІ та активною участю державних структур.

Зазначимо, що проблеми інформаційної та кібернетичної безпеки із суто спеціальних перетворилися на соціальні, себто перейшли у сферу захисту прав людини. Цілком очевидно, що виконувати інформаційно-захисні функції, гарантувати дотримання прав особи й суспільства в цій сфері має передовсім держава за допомогою законодавства. Вважаємо, що задля захисту прав людини й суспільства у боротьбі зі правопорушеннями у кібернетичному просторі, комп'ютерними злочинами потрібна не лише уніфікація відповідного національного законодавства, а й вироблення єдиних підходів на міжнародному рівні, об'єднання зусиль усієї світової спільноти щодо регулювання процесів користування глобальним кіберпростором.

Водночас державна політика забезпечення кібернетичної безпеки має спрямовуватися на мобілізацію системи освіти, засобів масової інформації на популяризацію, пропагування морально-етичного поводження в кіберпросторі, глобальній електронній мережі, формування у суспільній свідомості відповідних поведінкових моделей, котрі врешті-решт мають створити базис системи інформаційної та кібернетичної безпеки.

У руслі аналізованих вище питань інформаційної безпеки приєднуємося до позиції американського професора філософії Т. Байнума, котрий у контексті розв'язання сучасних проблем застосування новітніх технологій визначає певні рівні, ступені поширення етичних знань (Bynum, 1999, с. 32).

На першому – базовому – рівні до всіх суб'єктів спільноти доводиться істина про соціальні й морально-етичні наслідки використання інформаційних технологій та кіберпростору. Робиться це шляхом якнайширшого інформування суспільства стосовно проблематики, пов'язаної із створенням і застосуванням новітніх технологій, популяризації та пропаганди відповідної поведінки. На цьому рівні інформаційної етики одну з головних ролей відіграють засоби масової інформації. Стосовно проблем сфери інформаційної безпеки, відповідних прав і обов'язків її суб'єктів постійно, в міру зростання впливу новітніх технологій, має сповіщати населення система розповсюдження інформації. Широкий загал маж чітко усвідомлювати, які переваги й водночас загрози несе поширення інформаційних технологій та використання кіберпростору. На нашу думку, позитивним результат такої діяльності на першому рівні популяризації інформаційної етики та інформаційної безпеки можна вважати тоді, коли зростатиме кількість соціальних суб'єктів інформаційних відносин, котрі будуть спроможні попередньо оцінювати поведінку інших суб'єктів цих стосунків, виявляти та розпізнавати соціальні та морально-етичні проблеми, що водночас виникають, будучи до того ж пересічними громадянами, не фахівцями у дотичних сферах – кібернетики, інформаційних технологій, філософії, соціології, правознавства та ін.

Другий рівень інформаційної етики – теоретичний. Тут до аналізу соціально-етичних проблем суспільства, пов'язаних з використанням інформаційних технологій і кібернетичного простору, поєднується теоретичний пошук. На наше переконання, оскільки теоретична інформаційна етика дає змогу фахівцеві розглядати морально-етичні ситуації, що виникають, використовуючи для наукового пошуку та всебічного аналізу нагальних проблем філософський, соціологічний, юридичний та інший дослідницький інструментарій, дисципліна «теорія інформаційної етики» має увійти в навчальні плани вищих закладів освіти.

Звісно, вказані рівні поширення морально-етичного знання тісно взаємопов'язані й не мають чіткого розмежування. Об'єднує їх спільна надмета – захист загальнолюдських цінностей, прав і свобод людини і громадянина. Відтак, кожен соціальний суб'єкт і, відповідно, суспільство загалом мають усвідомити усі можливі наслідки – позитивні й негативні – користування інформаційними технологіями й кібернетичним простором. Тому ІТ-фахівці, державні, політичні й громадські діячі, аби їхня діяльність була ефективною, мусять володіти знаннями й навичками, які б відповідали принаймні другому рівню інформаційної етики. Водночас завданням наукової спільноти у своїх дослідженнях є подальше розкриття соціального й морально-етичного впливу інформаційно-телекомунікаційних технологій та використання кіберпростору.

З огляду на це одним із пріоритетів державної політики у сфері забезпечення кібернетичної безпеки має стати сприяння й усебічна підтримка наукового пошуку, пов'язаного з розробкою та впровадженням новітніх цифрових технологій, аналітичних і прогностичних досліджень у цій галузі (Лук'янчук, 2015: 112). Водночас, як убачається, вказані дослідження, котрі базуються на положеннях інформаційної етики, мають спрямовуватися на синтез набутого досвіду, моделювання теоретичних концепцій, напрацювання рекомендацій щодо налагодження оптимальної системи інформаційної та кібернетичної безпеки, а також на прогнозування можливих негараздів від використання комп'ютерних технологій, їх попередження, нейтралізацію та знешкодження.

Важливим чинником розроблення наукового підґрунтя кібернетичної безпеки є також:

– розроблення освітніх методик у цій галузі та механізмів формування під час освітнього процесу інформаційної культури;

– сприяння розробленню та поширенню наукових, науково-популярних, навчальних, методичних, довідкових та інших матеріалів стосовно питань інформаційної та кібернетичної безпеки, культури та етики особи й суспільства;

– підготовка й підвищення кваліфікації педагогічних працівників з метою налагодження в системі вищої, спеціальної та середньої освіти високопрофесійного навчального процесу для підготовки високопрофесійних кадрів системи забезпечення інформаційної та кібернетичної безпеки.

Водночас роль державних інститутів у забезпеченні процесів інформаційної взаємодії полягає насамперед в особливому сприянні, патронаті цієї сфери, але аж ніяк не жорстким контролем кожної її галузі чи стадії. На виконання своїх відповідних функцій державні структури мають виконувати такі завдання: формувати, проголошувати, популяризувати морально-етичні принципи, на яких базується інформаційне суспільства, а також надавати їм юридичної форми; здійснювати моніторинг і контроль за їх утіленням й дотриманням; вживати відкритих і прозорих регулятивних заходів у разі відсутності підтримки вказаних принципів або ж зловживань з боку окремих суб'єктів.

Крім того, держава повинна втілювати в життя вказані морально-етичні регулятивні норми, прищеплювати повагу до них як до взірця етичного застосування інформаційних технологій і користування кіберпростором. У результаті впровадження інформаційної етики має посприяти утвердженню в свідомості суспільства тих принципів, на яких воно має будуватися на інформаційному етапі свого розвитку. Своєю чергою, ці принципи мають екстраполюватися на сферу захисту прав і свобод людини.

Водночас, як уже побіжно зазначалося, створювати оптимальне з морально-етичного погляду інформаційне середовище варто не тільки, ба навіть не стільки шляхом блокування й покарання порушників, скільки й передовсім – формуванням виховних зразків, розробленням і впровадженням методів і засобів, спрямованих на осягнення населенням морально-етичних цінностей, прищепленням поваги до них, а також до самоаналізу й самовдосконалення. Надметою усіх цих заходів є досягнення в інформаційному, кібернетичному середовищі морально-етичної саморегуляції та заснованого на спільних інтересах і соціальній відповідальності самоконтролю.

Спробуємо виокремити ті різновиди соціальних спільнот у сфері застосування інформаційних технологій і використання кіберпростору, які, на нашу думку, мають потребу в морально-етичному регулюванні.

Це, по-перше, професіонали, ІТ-спеціалісти, для яких ця галузь є сферою фахової діяльності. Сюди ж слід віднести й колективи, бізнес-інтереси котрих пов'язані з інформаційним, кібернетичним середовищем, а також віртуальних викладачів, бібліотечних працівників та деяких інших. До другого типу належать усі категорії індивідуальних й колективних користувачів. Спільноти третього типу складають засоби масової інформації. Нарешті, четвертий тип складається з тих, хто займається регулюванням контенту в інформаційному, кібернетичному просторі. Через брак правових важелів впливу для цієї категорії засобом забезпечення прозорості у роботі пошукових механізмів покликані слугувати морально-етичні кодекси.

Варто зазначити, що питання морально-етичного регулювання професійної діяльності вже доволі давно перебувають серед пріоритетів у середовищі ІТ-фахівців. Так, вельми вагомий внесок у справу підвищення професіоналізму й морально-етичного становлення комп'ютерних спеціалістів, прищеплення професійної відповідальності зробили етичні кодекси Інституту інженерів електротехніки та радіоелектроніки (IEEE, 1990 р.) та Асоціації виробників обчислювальної техніки (ACM, 1992 р.). Положення, закріплені в цих документах, свідчать про те, що фахівці прагнуть не лише керуватися загальноприйнятими в соціумі морально-етичними нормами, а й дотримуватися засадничих принципів інформаційної та кібернетичної безпеки, таких як таємниця відомостей, конфіденційність, доступність і достовірність інформації тощо.

Варто також додати, що в теперішній час усе більше актуалізується питання професійної відповідальності, що зумовлено підвищенням вимог до фахового рівня спеціалістів в умовах розвитку інформаційного суспільства й зростання уваги до інформаційної та кібернетичної безпеки.

Ще у 2003 році Р. Броді увів до наукового обігу таке поняття, як «інформаційна наївність» ІТ-професіоналів, доводячи кардинальну відмінність змісту слів «знати про» та «знати». Визначив він це поняття як «стан, який не може бути більшим, ніж реалізація процесу, пов'язаного з виробленням артефактів» (Brody, 2003, с. 34) Дещо розширюючи семантику «наївності» (щось безпосередньо просте, викликане життєвою недосвідченістю), додамо сюди брак професійних знань і умінь, а також невисокий рівень компетентності.

Вважаємо, що протидія такій професійній ваді полягає в активному застосуванні у професійній інформаційній, кібернетичній сфері морально-етичні кодекси, покликані запобігати можливим негативним проявам, формувати високу фахову компетентність, ретельність і відповідальність. Про ці речі нами вже описувалося у попередньому підрозділі.

Стосовно ж третьої категорії користувачів, діяльність яких в інформаційній сфері та кіберпросторі потребує регулювання, то слід підкреслити що формування професійної журналістської етики, працівників засобів масової інформації має давні традиції, тісно пов'язані із загальними світовими процесами демократизації й гуманізації. У теперішній час це – загальновизнані у професійному середовищі принципи міжнародної журналістської етики, котрі вимагають дотримуватися у роботі правдивості й об'єктивності, безкорисливості, поваги до гідності людини, до її приватності, виражати суспільні інтереси, загальнолюдські цінності, висвітлювати усе розмаїття культур та поглядів, а також діяти відповідно до норм інформаційної безпеки.

Нинішні досягнення інформаційно-телекомунікаційних технологій, охоплення ними усіх сфер людської життєдіяльності створюють для засобів масової інформації величезні потенції впливу на суспільну свідомість. Тому дуже важливо, щоби професійні журналісти усіх ЗМІ інтерполювали на глобальні інформаційні мережі та кіберпростір високі норми свого корпоративного етичного кодексу.

Нарешті, спільнота провайдерів інтернет-контенту – ще одна категорія, діяльність котрої через відсутність, як уже зазначалося вище, її правового регламентування, потребує обов'язкового, на наше переконання, запровадження морально-етичних кодексів. Питання, які треба передбачати в такому документі, повинні, на нашу думку, стосуватися, зокрема, підпорядкованості пошукових інтернет-служб, критеріїв блокування й поширення інтернет-контенту, гарантій їх етичної роботи та ін. Сюди варто віднести також питання відповідальності «регулювальників» всесвітньої мережі за ретранслювання в кіберпросторі незаконного, забороненого, шкідливого, небезпечного чи неетичного контенту.

У цьому контексті показовим убачається приклад, коли всесвітньо відома потужна компанія Google визнала, що під час панорамної зйомки вулиць населених пунктів для картографічного сервісу Street View її співробітники порушували вимоги недоторканності приватного життя. Фотографуючи міста, «гугломобілі» водночас «збирали персональні дані громадян у незашифрованих мережах Wi-Fi протягом кількох років. Ця інформація містила логіни, паролі, листи електронної пошти. У подібних порушеннях була також викрита компанія «Яндекс» (7).

Отже, убачається цілком очевидним, що інтернет-посередники мусять сповіщати про принципи, форми й методи своєї діяльності, гарантуючи при цьому дотримання конфіденційності довіреної їм інформації. Відтак, потреба обговорення й формування відповідного морально-етичного кодексу є вельми нагальною.

Окремі зразки таких зведень уже є. Це, наприклад, кодекс практики для виробників баз і банків даних, запропонований Європейською асоціацією з інформаційних послуг (EUSIDIC). У цьому документі червоною ниткою проводиться ідея дотримання повноти, достовірності, доступності, конфіденційності та інших принципів інформаційної безпеки. Його положення спрямовані на забезпечення відкритості інформаційних потоків з обов'язковим урахуванням вимог захисту персональних даних та законних інтересів усіх суб'єктів відносин, пов'язаних із виробництвом, зберіганням і переданням інформації. Упевнені, що міцним фундаментом професійної діяльності спільнот інтернет-провайдерів саме й мають стати принципи справедливості, відкритості, достовірності й конфіденційності. Про це наголошують і вітчизняні дослідники (Ткачук, 2019, с. 310).

Висновки. Підбиваючи певні підсумки, зазначимо, що мінімізація викликів і загроз в кібернетичному просторі, створення безпечних умов життєдіяльності в інформаційному суспільстві потребують значних зусиль від усіх суб'єктів відповідних відносин. У цьому контексті потреба запровадження соціальних заходів забезпечення інформаційної та кібернетичної безпеки як принципово нової форми захисту цієї сфери якраз і зумовлена зростанням ролі в ній соціального складника. Тож із цією метою розроблено комплекс освітніх та виховних заходів, широка інформаційно-пропагандистська кампанія за активної участі, зокрема, державних інститутів із залученням якнайширшого числа усіх категорій засобів масової інформації та новітніх технологій для популяризації в суспільній свідомості зразків, форм і способів моральної поведінки у глобальному інформаційному та кібернетичному просторі. Ключовим складником цієї кампанії вбачається розгортання наукового пошуку в межах інформаційної етики – галузі етичної науки, котра проходить етап свого становлення й розвитку.

Соціальні інформаційно-безпекові заходи утворюють складну, багаторівневу систему, спрямовану на забезпечення інформаційної та кібернетичної безпеки на трьох рівнях – макро- (усе суспільство), мезо- (соціальні спільноти, організації тощо) та мікро- (індивідууми).

Головними суб'єктами захисту на першому рівні є суспільство й держава, задля забезпечення безпеки котрих у рамках реалізації відповідної державної політики належить, насамперед, сформувати несуперечливу концепцію правового забезпечення інформаційно-безпекової сфери. По-друге, треба всебічно популяризувати, за активної державної підтримки та участі, основні положення інформаційно-кібернетичної безпеки, права й обов'язки у цій сфері. Нарешті, необхідне створення міцних теоретичних, методологічних засад у сфері інформаційної та кібернетичної безпеки.

На другому, середньому, або мезорівні технологіями захисту його суб'єктів (соціальні групи, громадські, релігійні та інші організації чи об'єднання, професійно-виробничі структури тощо) є усталені та прийняті в різноманітних соціальних чи професійних спільнотах морально-етичні норми та правила безпечного користування інформаційними технологіями та кіберпростором, приписи та процедури взаємодії у вказаній сфері.

На індивідуальному, мікрорівні соціальних інформаційно-безпекових заходів вони втілюються шляхом просвіти, навчання й виховання індивідів задля формування в його свідомості системи правових і морально-етичних регуляторів, відповідних алгоритмів та інструментів, котрі визначають їх поведінку при використанні інформаційних технологій та кіберпростору.

Узагальнюючи аналіз соціальних інформаційно-безпекових заходів, зазначимо, що це – багаторівневий технологічний комплекс, який ухвалений державою і підтримується особою, колективом, групою та суспільством, спрямований на формування в суспільній свідомості специфічного механізму регулювання моральної поведінки людей у процесі користування інформаційними технологіями та кіберпростором, дотримання морально-етичних вимог в інформаційних соціальних відносинах.

Список використаних джерел:

1. Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Моніторинг рівня кібербезпеки України у світових рейтингах. *Інформаційна безпека людини, суспільства, держави*. Київ: Національна академія Служби безпеки України. 2019. №3(27). С. 100–107.
2. Bynum T. The Development of Computer Ethics as a Philosophical Field of Study. *The Australian Journal of Professional and Applied Ethics*. 1999. № 1(1).). P. 31-42.
3. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник Національної академії державного управління при Президентові України*. 2015. № 3. С. 110-117.
4. IEEE. Офіційний вебсайт. URL: https://www.ieee.org.
5. Association for Computing Machinery. Офіційний веб-сайт. URL: https://www.acm.org.
6. Brody R. Information ethics in the design and use of metal. IEEE Technology and Society Magazine. 2003. Vol. 22(2). P. 34.
7. Обшуки в Яндекс: за ким шпигувала російська компанія. URL: https://politeka.net/uk/news/443162-obyski-v-yandeks-za-kem-shpionila-rossijskaya-kompaniya-video.
8. EUSIDIC. Официальный сайт. URL: http://www.eusidic.org.
9. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис.... д. ю. н.: 12.00. 07. Ужгород. 2019. 487 с.

References:

1. Trofymenko O.H., Prokop Yu.V., Lohinova N.I., Zadereiko O.V. (2019) Monitorynh rivnia kiberbezpeky Ukrainy u svitovykh reitynhakh [Monitoring the level of cybersecurity of Ukraine in world rankings]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy*. Kyiv: Natsionalna akademiia Sluzhby bezpeky Ukrainy. №3(27). S. 100–107.
2. Bynum T. (1999) The Development of Computer Ethics as a Philosophical Field of Study. *The Australian Journal of Professional and Applied Ethics*. № 1(1).). P. 31-42.
3. Lukianchuk R.V. (2015) Derzhavna polityka u sferi zabezpechennia kibernetychnoi bezpeky v umovakh provedennia antyterorystychnoi operatsii [State policy in the field of cyber security in the context of an anti-terrorist operation]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy*. № 3. С. 110-117.
4. IEEE. Official website. URL: https://www.ieee.org.
5. Association for Computing Machinery. Official website. URL: https://www.acm.org.
6. Brody R. (2003) Information ethics in the design and use of metal. IEEE Technology and Society Magazine. Vol. 22(2). P. 34.
7. Searches in Yandex: who was spying on the Russian company. URL: https://politeka.net/uk/news/443162-obyski-v-yandeks-za-kem-shpionila-rossijskaya-kompaniya-video.
8. EUSIDIC. Official website. URL: http://www.eusidic.org.
9. Tkachuk T.Y. (2019) Pravove zabezpechennia informatsiinoi bezpeky v umovakh yevrointehratsii Ukrainy [Legal provision of information security in the conditions of Ukraine's European integration]: dys.... d. yu. n.: 12.00. 07. Uzhhorod. 487 s.