О. В. Соснін,
доктор політичних наук, професор,
заслужений діяч науки і техніки України,
Інститут держави і права ім. В. М. Корецького
Національної академії наук України

УДК: 378.046-021.68:37.014.6

ДО ПИТАННЯ ПРОТИДІЇ СТІЙКОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИМ ЗАГРОЗАМ

Немає сумніву в тому, що світ цифрових технологій, у який ми входимо, — це не тільки новий логічний етап розвитку технологічної сфери людства, а й усієї правової і соціально-політичної реальності. Поки ще не існує загальноприйнятих і гармонізованих визначень і правових дефініцій, однак, цифрові технології вже стрімко захоплюють плацдарми для наступу. Цифровізація (англ. digitalization) стає найважливішим фактором економічного зростання економіки будь-якої країни. Цифровізація є сучасним трендом розвитку і послідовного покращення всіх бізнес-процесів економіки і пов'язаних з нею соціальних сфер, заснованим на збільшенні швидкості взаємного обміну, доступності і захищеності інформації. Експерти виділяють вісім основних пунктів економічної системи цифрової економіки, як-то: держава і суспільство, маркетинг і реклама, фінанси і торгівля, інфраструктура і зв'язок, медіа і розваги, кібербезпека, освіта і кадри, стартапи й інвестиції. Виходячи з цього, при визначенні основних цілей розвитку цифрової економіки можна виділити: розумні міста, автономний транспорт, захист від кібератак, відповідальне ставлення до персональних даних, усунення цифрової нерівності, телемедицина, розумне сільське господарство, механізми довіри в Internet. Упровадження в життя будь-яких нових технологій — процес, безумовно, тривалий і несе купу ще невідомих викликів та небезпек для людства, їх зазвичай об'єднують у три різні групи: соціально-економічні, техніко-організаційні, природні. Усе це достатньо повно ми усвідомили в XX ст., впроваджуючи в реальну економіку науково-технічні досягнення через розробку нормативно-правових чинників (закони про працю, природоохоронне законодавство, правила, норми, стандарти, практика державного і суспільного контролю за їх дотриманням). Розвиток масового (конвеєрного) виробництва свого часу взагалі стимулював глибоке вивчення соціальних і правових питань реальної економіки — адекватної платні за працю, системи пільг і компенсацій, морального і матеріального стимулювання за шкідливі умови праці тощо. Запозичивши досвід Г. Форда, ми почали вивчати соціально-психічні чинники, що характеризують ставлення людини до праці, психологічний клімат у колективі, сім'ї, мотиви до праці; суспільно-політичні чинники — створення сприятливих умов праці, до винахідництва і інноваційної діяльності.

Ми запам'ятали, що за відсутністю правових норм і законів завжди існує вірогідність прояву небезпеки, що стало аксіомою небезпеки, що в природі немає абсолютно безпечних для життя людини явищ, факторів — все небезпечно і вимагає формування певних умов для роботи. Ми запам'ятали також, що існує багато прикладів, коли недостатність знань і нестача методологічно опрацьованих наукою і освітою обґрунтувань при практичному впровадженні знань і технологій у реальну економіку призводить до серйозних інженерно-технічних і гуманітарно-освітніх проблем і навіть до катастроф. Разом із тим, вступаючи в електронну еру, ми винятково легковажно поставилися до правових питань визначення фундаментальних понять «інформація», «інформаційний ресурс», «інформаційна безпека» тощо.

Ключові слова: *інформація, інформатизація, інформаційно-комунікаційні технології, інформаційно-комунікаційна безпека, інформаційно-комунікаційна діяльність, інформаційний простір, інформаційна війна, гуманітарні науки, наукова та освітня політика, інформаційне законодавство.*

Аналіз глобальних тенденцій XXI ст. дозволяє стверджувати, що подальший розвиток держав буде відбуватися за умов величезних технологічних і психоемоційних викликів і ризиків. На цих засадах вже сьогодні відбувається становлення суспільств, їх політики, військової справи і, безумовно, науки й освіти. Ризики стали фундаментом принципово нової економіки (knowledge-based economy), основою конкурентоспроможності країн, де створюються нові проривні технології надвисокого рівня (high-tech).

Нечуваним тріумфом науки XX ст. стало те, що людство, використовуючи сучасні ІКТ, розширило значення інформації як ресурсу розвитку країн, збільшило значення інтелектуальних можливостей громадян. У XXI ст. Internet та інші взаємопов'язані мережі (кіберпростір) підсилили значення науки і освіти, стали вкрай важливими для життя людини та її політичної незалежності.

Разом із тим, неврегульованість багатьох політико-правових питань, пов'язаних із інформаційно-комунікаційною сферою, набула ознак небезпеки, оскільки у світі відбулося сильне зростання значення комунікації — взаємозв'язків, а ризики і загрози тут виявилися настільки складними і всеосяжними, що їх рівень зростає за логарифмічною прогресією в порівнянні з можливістю протистояти їм за допомогою норм чинного права.

До того ж в умовах світової інформаційно-комунікаційної революції норми інформаційно-комунікаційного права сприймаються у нас поки що без належної уваги і критичного аналізу, іноді просто ігноруються, і все це на тлі досягнень науково-технічного прогресу, який уже надав необмежені можливості урядовим і неурядовим структурам контролювати і керувати за допомогою інформаційних впливів свідомістю і поведінкою людей — і простих громадян, і президентів країн. Державні органи мають здійснювати розробку загальних принципів політики у сфері цифрової економіки, що стосуються всіх секторів економіки, які спрямовані на досягнення стійкого економічного зростання, а також мають аналізувати проблеми, що виникають унаслідок цифрової трансформації, ризики і ефекти цифровізації економіки, в тому числі пов'язані з забезпеченням кібербезпеки, зайнятістю населення і забезпеченням громадян навичками і знаннями, які є необхідними в умовах цифрової економіки. Особливу увагу треба присвятити моніторингу й оцінці результативності й ефективності заходів політики цифровізації економіки. Сьогодні в політиці провідних країн світу спостерігається перехід до комплексного цифрового порядку, основною метою якого є: цифрова трансформація державного управління, розвиток інформаційно-комунікаційної інфраструктури на підґрунті нових цифрових технологій, укріплення кібербезпеки, розвиток цифрових навичок і компетенцій. Крім цього, розробляються стратегії впровадження окремих цифрових техно-

логій з високими потенційними ефектами в різних секторах економіки.

З точки зору безпеки, будь-який вид електронної комунікації виключно вразливий — за допомогою технічних засобів із комп'ютерів можна зняти будь-яку інформацію. Існують, звичайно, способи захисту, але стовідсоткової гарантії, що вони спрацюють, немає. Загрозою є не тільки те, що спецслужби країн світу сьогодні здатні підключатися і «знімати» за допомогою технічних засобів інформацію навіть із оптоволоконних (цифрових) кабелів. Вільний ринок технічних засобів надає доступ до величезних обсягів даних через електронну комунікацію іноземним розвідкам і кримінальним структурам, що постійно продукує нові загрози й виклики. Добуваючи інформацію, державні і приватні спецслужби досягли такого рівня, що здатні «зламувати» не тільки канали зв'язку, комп'ютерних мереж, але й людський мозок. Технічно їм для цього потрібні лише дві речі: велика обчислювальна потужність — певний обсяг персональних даних, зокрема, біометричних. До сьогодні ні в кого, крім спецслужб, не було такої мотивації, однак, ситуація змінюється через поліпшення ефективності машинного навчання, штучного інтелекту, розвитку психології, біології, зокрема нейробіології, необхідних для розуміння того, як працює людський мозок. За таких умов виникає необхідність забезпечення безпеки основних інструментів цифрової економіки — захист електронного підпису, електронних платежів, токенів, sim-карт, online-сервісів, захист інформації в електронних хмарах, базах даних, розвиток криптографії і технологій аутентифікації особи, захист системи електронного документообігу, каналів передачі інформації, захист серверів, безпеку діяльності комерційних і державних електронних майданчиків, захист від кіберзагроз безпілотних літальних апаратів і транспорту, новітніх технологій тощо.

Робота з інформацією в цифровому вигляді у світі набуває ознак величезної проблеми, що навіть створює ілюзію щодо недоцільності подальшої розбудови інформаційного суспільства, оскільки цифрова інформація дедалі більше набуває ознак зброї проти людства — її й виділяють саме як зброю інформаційних війн, що стимулює розвиток інформаційного права як науки і навчальної дисципліни в університетах.

Інформаційна зброя як сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційно-комунікаційну сферу супротивника з метою руйнування його інформаційної інфраструктури, систем управління державою, зниження працездатності громадян і військових, поки що не знаходить визначення в українському законодавстві.

За таких умов під суттєвою загрозою опиняються об'єкти критичної інфраструктури держави (енергетика, транспорт тощо). Інформація, яку ми вільно використовуємо в повсякденному житті, в цифровому вигляді несе в собі всі ознаки, що характеризують її як зброю:

— інформація може надаватися в сучасному світі як один з найбільш необхідних, затребуваних, дорогих і максимально захищених ресурсів;

— інформація стає засобом інформаційного протиборства в руках політичних структур, релігійних сект, терористичних груп і навіть держав;

— вільний доступ і відсутність дієвого контролю, вразлива в багатьох аспектах система захисту серверів від несанкціонованого доступу дозволяють самовільно знімати інформацію, поширювати неправдиві відомості, передавати і отримувати секретні матеріали, блокувати канали надходження програм або самовільно переадресовувати їх;

— інформацію можна розглядати як з точки зору психологічного, так і з точки зору технічного впливу;

— інформація має унікальні властивості, що дозволяють вважати її високоефективною зброєю: скритність, масштабність і універсальність;

— поряд із впливом на засоби масової інформації та телекомунікацій, одним із головних об'єктів впливу інформаційної зброї залишаються люди, їх світогляд.

Вищезазначеного не внесено відповідним чином до нормативно-правових актів України. Так само, як і сам термін «інформаційна війна», який з'явився в другій половині XX ст. в США. У військових колах під інформаційною війною розуміються дії, що вживаються для досягнення інформаційної переваги в підтримці національної військової стратегії за допомогою впливу на інформацію та інформаційні системи супротивника при одночасному забезпеченні захисту і безпеки власної інформації та інформаційних систем з метою:

— контролювати глобальний інформаційний простір, захищаючи при цьому свою інформацію від ворожих дій (контрінформація);

— використовувати контроль за інформацією для ведення інформаційних атак на супротивника;

— підвищувати загальну ефективність власних збройних сил за допомогою повсюдного використання військових інформаційних функцій.

Складові частини інформаційної війни:

— психологічні операції — використання інформації для впливу на аргументацію солдатів ворога;

— електронна війна — не дозволяє ворогові отримати точну інформацію;

— фізичне руйнування — може бути частиною інформаційної війни, якщо має на меті вплив на елементи інформаційних систем;

— заходи безпеки — захист своєї інформації;

— прямі інформаційні атаки — пряме перекручування інформації без видимої зміни сутності, в якій вона знаходиться.

Реклама, пропаганда, дроблення та фрагментація, перехоплення інформації, вміння її спотворювати — все стає зброєю (для застосування цих методів використовують різноманітні технічні і технологічні засоби — супутники, радіорелейні лінії, Internet, електронну пошту, звичайні засоби масової інформації). Лише однією з технологій віртуалізації нашого життя є широко рекламований міф, який необачно легко пропонує масову комп'ютеризацію суспільства та перетворення інформації у вирішальний фактор життя суспільства.

За таких умов масова неконтрольована нормативно-правовими актами інформатизація суспільства стає дедалі більшою загрозою з точки зору організації сучасного життя в державі. Рівень відповідальності влади щодо впровадження в усі сфери людської діяльності ІКТ і засобів електронно-обчислювальної техніки зростає, а інформація та інформаційні ресурси стають одним із вирішальних факторів розвитку особистості, суспільства і держави. І хоча широкі можливості комп'ютерів та інформаційно-комп'ютерних технологій (ІКТ) дозволяють активізувати демократичні засади розбудови суспільства, полегшити (автоматизувати) процеси моніторингу й управління державними, економічними, соціальними, оборонними та іншими об'єктами й системами з метою своєчасно отримувати, накопичувати, обробляти і передавати інформацію практично з будь-якою необхідною швидкістю і в будь-якій кількості, суспільство має контролювати процеси інформатизації більш ретельно. Усе це не дає підстав стверджувати, що інформатизація відіграє сьогодні дещо негативну роль у розвитку людства, що інформаційне суспільство об'єктивно неминуче, але за умов адекватного розвитку громадянського. Історія вчить нас, що орієнтація виключно на переможну ходу досягнень науково-технічного прогресу не веде до гармонійного розвитку суспільства. От і сьогодні, набуваючи ознак головного ресурсу розвитку людства, інформація та ІКТ за відсутністю збалансованих норм права дедалі більше починають виступати як об'єкти загроз, які породжують глобальну проблему інформаційної безпеки особистості, суспільства й держави. Так, державній безпеці цифрова революція загрожує в наступних напрямах:

— кіберзлочинність, а саме кібертероризм і кібершпіонаж, що ведуться іншими країнами та іноземними терористичними та злочинними організаціями, а також окремими особами і групами осіб. Окрім того, слід виділити ті ж за-

грози, але з боку внутрішніх злочинних угруповань і терористичних організацій. Традиційною метою хакерських угруповань також є розкрадання фінансових коштів як з рахунків громадян, так і юридичних осіб;

— відхід від оподаткування, незаконне вивезення капіталу, відмивання злочинно отриманих доходів з використанням криптовалюти;

— здійснення незаконної підприємницької діяльності за допомогою використання мережі Internet, включаючи електронну торгівлю і фінансові послуги, поява нових можливостей для незаконної фінансової діяльності. У даному випадку йдеться й про поширення технології блокчейн, що може спричинити втрату державою монополії на емісію національної валюти.

У сучасних умовах національний цифровий простір, по суті, стає елементом критичної інфраструктури. Деякі негативні наслідки розвитку цифрової економіки для суспільства, особистості й бізнесу наведені нижче:

— технологічна вразливість створеної цифрової інфраструктури. З розвитком цифрової економіки, чим «розумнішими» стають пристрої доступу, тим потенційно вищим стає рівень вразливості власника. Поширення Internet-речей робить людину фактично «прозорою» для будь-яких зацікавлених осіб і структур, що, в свою чергу, породжує попит на розвиток технологій інформаційної безпеки і технологій кіберзлочинності;

— зростання технологічної залежності України від зарубіжних постачальників, і, як наслідок, ослаблення технологічної та економічної безпеки на рівні як країни в цілому, так і окремих галузей і підприємств;

— підвищення ризиків витоків різноманітної інформації;

— швидке старіння техніки, і, як наслідок, проблема її утилізації. Поки проблема поводження з «електронними відходами» не перебуває в центрі суспільної уваги. Тим часом, за даними ООН, щороку в світі утворюється до 100 млн тонн «електронних відходів», і тільки трохи більше 20% цього обсягу переробляється відповідно до екологічних вимог. Із розвитком цифрової економіки її небезпечні екологічні наслідки будуть наростати;

— зникнення (перш за все, в розвинених країнах) ряду масових традиційних професій, що може призвести до значного безробіття і соціальної напруги в суспільстві. У доповіді «The Future of Jobs», випущеній 17 вересня 2018 року Всесвітнім економічним форумом у Давосі, вказується, що до 2020 року нові технології знищать близько 5 млн робочих місць, через що зросте безробіття. [2] Широка автоматизація призводить до відмови від використання «живої» праці, що спричинить масові звільнення працівників. За окремими прогнозами, зі збільшенням безробіття сукупні доходи суспільства зменшаться, зростання заробітної плати зупиниться, наслідком чого стане скорочення сукупного попиту. У свою чергу, депресивний попит підірве стимули до інвестування і працевлаштування, наслідками чого стануть уповільнення зростання продуктивності і зниження загального добробуту суспільства;

— на рівні особистості — скорочення особистого простору;

— маніпулювання громадською думкою;

— загострення конкуренції і витіснення з ринку окремих гравців. Уже сьогодні IT-компанії випереджають сировинні за показником ринкової капіталізації. Відзначається, що в найближчі п'ять років цифрова революція витіснить з ринку 40% компаній, які зараз займають позиції лідерів галузі, положення в галузі, якщо вони не піддадуться цифровій трансформації.

Таким чином, цифрова економіка поряд з величезними можливостями, які вона надає для розвитку суспільства і бізнесу, також несе загрози, перш за все, для економічної та національної безпеки держави.

Сьогодні, коли ІКТ проникають в усі сфери життєдіяльності людини, інформація у цифровому вигляді унаявлює всі

відомості про навколишній світ, про процеси, що відбуваються в ньому і сприймаються людиною, живими організмами, керуючими машинами та інформаційно-комунікаційними системами.

Хоча саме поняття «інформація» почали розглядати і вивчати філософи ще з античних часів, цифрова інформація сприймається дещо інакше і є одним з найнеобхідніших продуктів життєдіяльності сучасного суспільства, а тому безпека може бути забезпечена виключно при системному комплексному політико-правовому підході. Інформаційно-комунікаційне середовище, в якому ми існуємо, представляється як сукупність цифрової інформації, яка нас оточує незалежно від форми її подання (письмової, усної, графічної).

Інформаційно-комунікаційне середовище має дві складові: інформаційно-технічну (штучно створену людиною — світ техніки, технологій тощо) та інформаційно-психологічну (світ живої природи, який включає і саму людину). Як наслідок, у загальному випадку інформаційну безпеку особистості, суспільства (держави) можна представити двома складовими частинами: інформаційно-технічною безпекою і інформаційно-психологічною (психофізичною) безпекою. Підвалини проблеми було закладено і зафіксовано ще в 1948 році у Загальній декларації прав людини (прийнята на третій сесії Генеральної Асамблеї ООН резолюцією 217 А (III) від 10 грудня 1948 року), в ст. 19 якої зазначено: «Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів».

Масова глобальна інформатизація України оголила всі ці питання, винесла їх на поверхню і, з одного боку, сьогодні дійсно сприяє інтелектуалізації людської діяльності, формуванню в національних державах наднаціональних структур щодо їх вивчення, але, як і будь-який процес, привела суспільство до певних небезпек і загроз в інформаційно-комунікаційній сфері, і тому забезпечення безпеки в інформаційно-комунікаційному середовищі стає пріоритетним напрямком науково-технічної діяльності, вимагаючи істотної уваги і зусиль з боку людини, суспільства, владних структур і юридичної науки держави.

Сьогодні інформаційно-комунікаційна безпека особистості, суспільства й держави визначається рядом ключових понять, які треба терміново оформлювати нормами права, як-то:

— інформаційна загроза — потенційна можливість певним чином порушити інформаційну безпеку. Найчастіше ця загроза, яка є наслідком наявності вразливих місць у захисті інформаційних ресурсів або систем при спробі реалізації інформаційної загрози називається інформаційною атакою;

— інформаційна небезпека — обставини, за яких інформація або її похідні можуть вплинути на людину або обставини таким чином, що це призведе до її виправлення або спотворення, тобто унеможливлення її подальшого функціонування й розвитку в позитивному напрямку. Під інформаційною небезпекою можна розуміти і появу відчутної ймовірності настання небажаних подій;

— інформаційний захист — процес забезпечення безпеки інформації. При цьому варто розуміти, що при якісному забезпеченні процесу захисту безпека буде забезпечена (або зведені до мінімуму небезпеки та загрози);

— інформаційна безпека особистості — це стан й умови життєдіяльності особистості, за яких реалізуються її інформаційні права і свободи. До життєво важливих інтересів особистості в інформаційній сфері відносяться: дотримання і реалізація конституційних прав на пошук, отримання, виробництво й поширення інформації; використання інформації з метою духовного, фізичного, інтелектуального розвитку; захист прав на об'єкти інтелектуальної власності; забезпечення прав громадянина на захист свого здоров'я від неусвідомлюваної людиною шкідливої інформації;

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

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

— інформаційна війна — використання й управління інформацією з метою отримання конкурентної переваги над противником. Інформаційна війна може включати в себе збирання інформації з метою її викривлення або спотворення в процесі пропаганди потрібних для перемоги дій та дезінформації з метою деморалізації противника;

— інформаційний тероризм — гранично небезпечне соціально-політичне явище, яке виникло як наслідок дій розвідок, спрямоване на дезорієнтацію свідомості людей з метою деструктивних видозмін знань та світогляду;

— інформаційна залежність — залежність від різних джерел інформації, нав'язливе бажання отримувати інформацію будь-якою ціною, хвороблива нездатність відмовитися від безперервного отримання інформації.

Питанням інформаційно-комунікаційної безпеки присвячується все більша кількість досліджень, в яких існує безліч трактувань самих термінів «інформаційна безпека», «комунікаційна безпека» або «інформаційно-комунікаційна безпека». Дані терміни в різних контекстах вживаються по-різному та мають різний зміст, що, само по собі, стає величезною проблемою для юридичної науки, призначення якої й полягає в її вирішенні. Основним юридичним документом, що регулює сферу інформаційної безпеки в Україні, є Доктрина інформаційної безпеки України (затверджена Указом Президента України від 25 лютого 2017 року № 47/2017) (далі — Доктрина інформаційної безпеки), яка достатньо повно визначає інформаційну безпеку як стан захищеності національних інтересів в багатогранній і багатовимірній інформаційно-комунікаційній сфері.

Не важко помітити, що всі ці характерологічні особливості проблеми мають формальний характер, тобто стосуються тільки форм її існування, зовсім не торкаючись її сенсу, а, як відомо, розвиток можливий виключно за умов прогресу в розумінні сенсу, а не тільки форми. За цим, безумовно, стоїть зміна уявлень про соціальну реальність, оскільки проблема інформаційно-комунікаційної безпеки є сукупністю всіх суспільно-політичних відносин, які можуть усвідомлюватися або не усвідомлюватися, усвідомлюватися адекватно або неадекватно, поглинають фундаментальне право громадян на інформацію. На тлі цих тенденцій зовсім не випадково наприкінці XX ст. стали популярними мислителі, які поставили за мету знищити все, що було тут опорою людству. «Хибними» були оголошені такі поняття як народ, нація, клас, держава, родина, культура, розум, наука.

Різні популяризатори гуманітарних теорій «віртуальних світів» спираються при цьому на природничо-наукові теорії

«паралельних світів», коеволюції[1], забуваючи, що вчені при цьому зовсім не стверджували про одночасне існування кількох об'єктивних реальностей, що суперечило б самому принципу науковості, а розглядали свої теорії лише як різні моделі або сценарії. Філософи постмодерністської хвилі не зрозуміли свого часу повноти проблеми і сьогодні часто свідомо відмовляються від поняття об'єктивної реальності, стверджуючи абсолютний релятивізм і суб'єктивізм у пізнанні, але якщо визнання абсурду буття не залишається на рівні інтелектуальної гри, то його політизація, як правило, призводить до ідеології повного заперечення законів реального світу, що виявляється в реальній практиці в актах екстремізму й тероризму — закономірних підсумків використання етичного як політичного засобу.

Несправедливо сьогодні звинувачувати всіх у гонитві за матеріальними або віртуальними цінностями. Абсолютна більшість навчається й працює. У пошуках «свого» місця людина є дуже критичною, успадковуючи досвід минулого, часом категорично не сприймає його досягнень і навіть моралі. Вічний конфлікт «батьки і діти», заснований на споконвічній чистоті людської душі, як і сто-двісті років тому, так само входить у суперечність із «прозою» реального життя, до якої доросла людина звикла, але молода — ніколи. Тому й виглядає часом безапеляційною, часом агресивною, що є цілком закономірним.

Треба розуміти, що за останнє півстоліття масовій свідомості людини завдано непоправних морально-психологічних травм процесами «дикої» приватизації, масової інформатизації тощо. Людство взагалі, безсумнівно, усвідомлює глибину цих проблем, але набагато менше розуміє, що і як із цим робити, а це треба знати, розпочинаючи вирішення проблем інформаційно-комунікаційної безпеки. [3] Вони інтегрують у собі умови формування у свідомості людини правильних переконань, намірів, мови, поведінки, правил існування й організації своєї волі. [1]

Ще одним важливим аспектом розвитку права в сучасних умовах є те, що Всесвітня організація охорони здоров'я (ВООЗ) роботу з персональним комп'ютером віднесла до небезпечних, бо їй притаманний фактор постійно діючого стресу, через що небезпеці піддаються всі життєво важливі органи людини, з'являється ризик виникнення серйозних хвороб. Електромагнітні поля біля комп'ютера (особливо низькочастотні) негативно впливають на людину і, в першу чергу, на її центральну нервову систему, викликаючи головний біль, запаморочення, нудоту, депресію, безсоння, відсутність апетиту, виникнення синдрому стресу. Причому нервова система реагує навіть на короткі за тривалістю впливи слабких полів: змінюється гормональний стан організму, порушуються біоструми мозку. Це призводить до погіршення зору, ускладнення серцево-судинних захворювань, зниження імунітету, виникають негативні впливи на плин вагітності. Нерухома напружена поза оператора призводить до втоми і виникнення болю в хребті, шиї, плечових суглобах, а інтенсивна робота з клавіатурою викликає болючі відчуття в суглобах, зап'ястях і пальцях рук. При тривалій та інтенсивній роботі за комп'ютером з'являється синдром комп'ютерного стресу, який проявляється головним болем, запаленням очей, алергією, дратівливістю, млявістю й депресією, погіршенням зосередженості й працездатності.

Керуючись методами кібернетико-системного підходу, щонайпершим завданням правознавців стає проведення аналізу ряду кейсів технологічного вихован-

[1] У широкому сенсі, **біологічна коеволюція** (або **спряжена еволюція**) — це зміна біологічного об'єкта, викликана зміною пов'язаного з ним об'єкта, паралельна синхронна еволюція двох різних систем. Термін було застосовано екологами (П. Ерліхом, П. Рейвеном) в 1964 р. для опису координованого розвитку різних видів у складі однієї екосистеми (біоценозу). Концепція коеволюції використовується не лише в біології — також в екології, астрономії, створенні штучного життя та ін.

ня громадян своєї країни. Спочатку про затвердження в Китаї державного кібернетико-системного управління за допомогою big data — системи «соціального кредиту». У цій системі передбачається зовнішнє управління всіма соціальними сферами діяльності людей. Інший кейс — програмування сприйняття дійсності через сервіс «активний громадянин» — формально за своїм задумом має на меті процеси артикуляції громадської думки, а в реальності підміняє власні погляди й інтереси людей за допомогою різних технологій маніпуляції. [3] Другим завданням є, спираючись на дослідження і за допомогою феномен-соціологічного підходу, показати, як в internet-сфері відбувається прояснення в діалозі власних смислів людей як індивідуальних особистостей, а потім артикулюється на політичному рівні. Це в цілому служить розкриттю творчих можливостей особистості.

За таких умов сьогодні перед нами стоїть завдання навчитися по-новому регулювати нормами права інформаційно-комунікаційні відносини, які мають часто транскордонний характер, і врахувати необхідність формування у своїх громадян нового цілісного світогляду на основі світових тенденцій розвитку права, науки про державне управління, і, безумовно, певної віртуалізації уявлень філософів та психологів на нову реальність електронної доби розвитку.

Список використаної літератури

1. Бех І. Д. Від волі до особистості. Київ: Україна Віта, 1995. 202 с.

2. Бехер В. В., Зеленых Е. В. Цифровые технологии: угрозы и риски внедрения. URL: https: // esa-conference.ru/wp-content/uploads/files/pdf/Beher-Veronika-Vissarionovna. pdf.

3. Соснін О. В., Гордієнко С. Г. Окремі елементи розробки нової інституціональної матриці розвитку України // Загальнонаціональний правовий тижневик «Юридичний вісник України» № 37 (1262) 13—19 вересня 2019 року. С. 12—13; № 38 (1263) 20—26 вересня 2019 року. С. 10—11.

References

1. Beh I. D. From Freedom to Personality. Kiev: Ukraine Vita, 1995. 202 P.

2. Becher V. V., Zeleny E.V. Digital technologies: threats and risks of implementation. URL: https: // esa-conference.ru/wp-content/uploads/files/pdf/Beher-Veronika-Vissarionovna. pdf.

3. Sosnin O. V., Gordienko S. G. Separate Elements of Developing a New Institutional Matrix for the Development of Ukraine // National Law Weekly Bulletin «Ukrainian Legal Bulletin» No. 37 (1262) September 13—19, 2019. P. 10—11.

Соснин А. В. К вопросу противодействия устойчивости информационно-коммуникационным угрозам.

Нет сомнения в том, что мир цифровых технологий, в который мы входим, — это не только новый логический этап развития технологической сферы человечества, но и всей существующей правовой и социально-политической реальности. Пока еще не существует общепринятых и гармонизированных определений и правовых дефиниций, однако, цифровые технологии уже стремительно захватывают плацдармы для наступления. Цифровизация (англ. digitalization) становится важнейшим фактором экономического роста экономики любой страны. Цифровизация является современным трендом развития и последовательного улучшения всех бизнес-процессов экономики и связанных с ней социальных сфер, основанным на увеличении скорости взаимного обмена, доступности и защищенности информации. Эксперты выделяют восемь основных пунктов экономической системы цифровой экономики: государство и общество, маркетинг и реклама, финансы и торговля, инфраструктура и связь, медиа и развлечения, кибербезопасность, образование и кадры, стартапы и инвестиции. Исходя из этого, при опреде-

лении основных целей развития цифровой экономики можно выделить: умные города, автономный транспорт, защиту от кибератак, ответственное отношение к персональным данным, устранение цифрового неравенства, телемедицину, разумное сельское хозяйство, механизмы доверия в Internet.

Внедрение в жизнь любых новых технологий — процесс, безусловно, длительный и несет в себе массу неизвестных еще вызовов и опасностей для человечества, их обычно объединяют в три разные группы: социально-экономические, технико-организационные, природные. Все это достаточно полно мы осознали в XX в., внедряя в реальную экономику научно-технические достижения через разработку нормативно-правовых факторов (законы о труде, природоохранное законодательство, правила, нормы, стандарты, практика государственного и общественного контроля за их соблюдением). Развитие массового (конвейерного) производства в свое время вообще стимулировал глубокое изучение социальных и правовых вопросов реальной экономики — адекватной оплаты труда, системы льгот и компенсаций, морального и материального стимулирования за вредные условия труда и т. п. Позаимствовав опыт Г. Форда, мы начали изучать социально-психические факторы, характеризующие отношение человека к труду, психологический климат в коллективе, семье, мотивы к труду; общественно-политические факторы — создание благоприятных условий труда, к изобретательству и инновационной деятельности.

Мы запомнили, что из-за отсутствия правовых норм и законов всегда существует вероятность проявления опасности, что стало аксиомой опасности, что в природе нет абсолютно безопасных для жизни человека явлений, факторов — все опасно и требует формирования определенных условий для работы. Мы запомнили также, что существует много примеров, когда недостаточность знаний и нехватка методологически обработанных наукой и образованием обоснований при практическом внедрении знаний и технологий в реальную экономику ведет к серьезным инженерно-техническим и гуманитарно-образовательным проблемам и даже катастрофам. Вместе с тем, вступая в электронную эру, мы исключительно легкомысленно отнеслись к правовым вопросам определения фундаментальных понятий «информация», «информационный ресурс», «информационная безопасность» и другие.

Ключевые слова: *информация, информатизация, информационно-коммуникационные технологии, информационно-коммуникационная безопасность, информационно-коммуникационная деятельность, информационное пространство, информационная война, гуманитарные науки, научная и образовательная политика, информационное законодательство.*

Sosnin A. V. To the issue of resistance to information and communication threats.

There is no doubt that the digital world we are entering is not only a new logical stage in the development of the technological sphere of humanity, but also of all existing legal and socio-political realities. While common and harmonized definitions and legal definitions do not yet exist, digital technologies are already rapidly gaining ground for offensives. Digitalization is becoming a major factor in the economic growth of any country's economy. Digitization is a modern trend for the development and consistent improvement of all business processes in the economy and related social spheres, based on increasing the speed of mutual exchange, accessibility and security of information. The experts highlight eight key points of the digital economy: the state and society, marketing and advertising, finance and commerce, infrastructure and communications, media and entertainment, cybersecurity, education and human resources, startups and investments. Therefore, in determining the main goals of the digital economy can be identified: smart cities, autonomous transport, protection against cyberattacks, responsible attitude to personal data, elimination of digital

inequality, telemedicine, smart agriculture, mechanisms of trust in the Internet.
The implementation of any new technologies, the process, of course, is long and carries many unknown yet challenges and dangers to humanity, they are usually combined into three different groups: socio-economic, techno-organizational, natural. All this is quite fully understood in the twentieth century, introducing scientific and technological achievements in the real economy through the development of regulatory and legal factors (labor laws, environmental legislation, rules, norms, standards, practice of state and public control over their observance). The development of mass (conveyor) production of its time in general stimulated a deep study of social and legal issues of the real economy — adequate pay, a system of benefits and compensation, moral and material incentives for harmful working conditions and more. Borrowing the experience of G. Ford, we began to study the socio-psychic factors that characterize a person's attitude to work, psychological climate in the team, family, motives for work; socio-political factors for creating favorable working conditions, for invention and innovation.
We have remembered that in the absence of legal rules and laws, there is always a likelihood of danger, which has become an axiom of danger, that in nature there are no phenomena absolutely safe for human life, factors — everything is dangerous and requires the formation of certain working conditions. We have also remembered that there are many examples where a lack of knowledge and a lack of methodologically based science and education justification for the practical implementation of knowledge and technology into the real economy leads to serious engineering, humanitarian and educational problems and even catastrophes. And at the same time, entering the electronic era, we are extremely light-hearted in the legal issues of defining the fundamental concepts of «information», «information resource», «information security» and more.
Key words: *information, informatization, information and communication technologies, information and communication security, information and communication activity, information space, information war, humanities, scientific and educational policy, information legislation.*