ІНФОРМАЦІЙНА БЕЗПЕКА ТЕХНОЛОГІЙ МАЙБУТНЬОЇ ДЕРЖАВИ У ВИСОКОТЕХНОЛОГІЧНОМУ ГЛОБАЛЬНОМУ ПРОСТОРІ

INFORMATION SECURITY OF TECHNOLOGIES OF THE FUTURE STATE IN THE GLOBAL SPACE OF THE FUTURE

УДК 329.09.5

Мар'яненко Г.І.
к. наук з держ. упр.,
проректор з наукової роботи
Інститут підготовки кадрів державної служби зайнятості України

У статті здійснено аналіз інформаційної безпеки та загрози нових технологій у високотехнологічному просторі майбутнього в інформаційній сфері, яка має особливе значення для України і розвиток якої орієнтовано на комплексну інтеграцію у світове співтовариство, що неможливе без урахування інформаційного чинника. Це потребує замислення над перспективами розвитку інформаційного суспільства в Україні, для чого передусім необхідно визначити потреби, можливості та загрози щодо масового використання інформаційних технологій у світовому просторі. Нові інформаційні технології сьогодні стрімко проникають в усі сфери життєдіяльності нашого суспільства та дійсно фантастично змінюють нашу уяву про спосіб життя людини майбутнього, цей феномен вже сьогодні змінив життя сучасної людини. Нові технології стають причиною появи нових професій та зникнення професій, які майже сто років були затребувані ринком праці. Світове суспільство тільки намагається зрозуміти, які перспективи чи загрози нам несе інформаційно-технологічний простір майбутнього.
Ключові слова: *інформаційні технології, технології доповненої реальності (Augmented Reality – AR), штучний інтелект, інформаційна свідомість, інформаційний простір, інформаційні впливи, зовнішні загрози, спеціальні інформаційні операції, інформаційний суверенітет, інформаційна безпека.*

В статье осуществлен анализ информационной безопасности и угрозы новых технологий в высокотехнологичном пространстве будущего в информационной сфере, которая имеет особое значение для Украины и развитие которой ориентировано на комплексную интеграцию в мировое сообщество, невозможно без учета информационного фактора. Это требует задуматься о перспективах развития информационного общества в Украине, для чего в первую очередь необходимо определить потребности, возможности и угрозы для массового использования информационных технологий в мировом пространстве. Новые информационные технологии сегодня стремительно проникают во все сферы жизнедеятельности общества и действительно фантастически меняют наше представление об образе жизни человека будущего, этот феномен уже сегодня изменил жизнь современного человека. Новые технологии становятся причиной появления новых профессий и исчезновения профессий, которые почти сто лет были востребованы рынком труда. Мировое общество только пытается понять, какие перспективы или угрозы нам несет информационно-технологическое пространство будущего.
Ключевые слова: *информационные технологии, технологии дополненной реальности (Augmented Reality - AR), искусственный интеллект, информационная сознание, информационное пространство, информационные воздействия, внешние угрозы, специальные информационные операции, информационный суверенитет, информационная безопасность.*

The article analyzes the information security and the threat of new technologies in the high-tech space of the future in the information sphere, which is of particular importance for Ukraine, the development of which is focused on integrated integration into the world community, which is impossible without taking into account the information factor. This requires thinking about the prospects of the development of the information society in Ukraine, which first of all needs to identify the needs, opportunities and threats of the massive use of information technology in the world. New information technologies are rapidly penetrating into all spheres of life of our society and really fantastically change our imagination about the way of life of a person of the future, this phenomenon has today changed the life of modern man. New technologies are causing the emergence of new occupations and the disappearance of occupations that have been demanded by the labor market for almost a hundred years. The world community only tries to understand what prospects or threats we face with the information and technological space of the future.
Key words: *information technologies, technologies of augmented reality (AR), artificial intelligence, informational consciousness, information space, information influences, external threats, special information operations, information sovereignty, information security.*

Постановка проблеми у загальному вигляді. Питання інформаційної безпеки в інформаційній сфері має особливе значення для України, розвиток якої орієнтовано на комплексну інтеграцію у світове співтовариство, що неможливе без урахування інформаційного чинника. Це потребує переосмислення перспектив розвитку інформаційного суспільства в Україні та світі, для чого передусім необхідно визначити потреби й можливості щодо масового використання інформаційних технологій. Разом з тим необхідно враховувати, що саме інтенсивний розвиток інформаційних технологій призвів до нових загроз потенційного використання інформаційно-технічних досягнень у цілях, несумісних з підтримкою безпеки інформаційної сфери і стабільності функціонування сучасного суспільства. На цій підставі в умовах глобалізації інформаційного суспільства проблема інформаційної безпеки

в інформаційній сфері державного управління є актуальною і набуває соціально все більш значущого характеру [4].

Аналіз останніх досліджень і публікацій. Узагальнення результатів досліджень з питань розвитку та безпеки інформаційних технологій у різних галузях життєдіяльності суспільства, наукові досягнення та новітні відкриття світових вчених, демонструють що цій проблемі приділяло і приділяють увагу чимало учених: Ричард Броуді, Дуглас Рашкофф, Джон Маккарті, Ю. Поляков, М.А. Дмитренко та ін. Дослідження свідчать, що попри теоретичні та практичні досягнення вчених у сфері інформаційних технологій (ІТ), їх безпечного застосування у процесі формування високотехнологічного простору сьогодення і майбутнього є актуальним і потребує більш ґрунтовного вивчення.

Виділення невирішених раніше частин загальної проблеми. Оптимізація процесів розвитку інформаційних технологій, суспільних трансформацій і зовнішньополітичного механізму України вимагає чіткого перспективного бачення ролі й місця України у сучасному світі, аналізу динаміки її взаємодії з міжнародним середовищем у глобальному просторі, формування чіткої ґеополітичної стратегії державної інформаційної безпеки.

Мета статті. Головною метою цієї роботи є аналіз теорії та практики радикальної зміни соціальної диференціації інформаційного суспільства, поділ його не на класи, а на інформаційні співтовариства, що слабо диференціюються, це насамперед пов'язано з доступом до знань та інформації для широких верств населення. Знання перестають бути правом багатих, знатних та успішних. Між традиційними класами поступово «змиваються» межі (особливо це помітно у блогосфері). Об'єктивною основою об'єднання людей у постіндустріальному суспільстві стає розвиток освіти, науки, інформації.

Виклад основного матеріалу. Нові інформаційні технології розширюють і у той же час обмежують коло тих, хто має доступ до інформації. Постійний розвиток цифрового контенту підвищує важливість таких навичок інформаційної грамотності, як аналітичні здібності і вміння користуватися цифровими інструментами. Негативні – сьогодні ми спостерігаємо витіснення низькокваліфікованої праці (фізичної і розумової) машинами і появу нових видів компетенцій, що вимагають високої кваліфікації; морально-етичні проблеми у процесі взаємовідносин людина-машина; суперечності між можливостями людини сприймати та переробляти інформацію; інформаційний шум, надлишкова, зайва інформація; складність перевірки достовірності інформації та її безпека [8, с. 34].

Нині жодна сфера життя не тільки окремих суспільств і держав, але і усього світового співтовариства не може функціонувати без розвинутої інформаційної структури. Проникаючи в усі сфери діяльності держави, інформація здобуває конкретне політичне, матеріальне і вартісне вираження. Йде об'єктивний процес становлення інформаційного суспільства, в якому інформаційна діяльність буде основою економічного процвітання і добробуту. Однак саме через інформаційне середовище найчастіше здійснюються загрози національній безпеці у різних сферах діяльності держави [8, с. 26]. Негативні наслідки використання інформаційних технологій проявилися у збільшенні розриву між рівнями розвитку багатих індустріальних країн та іншого світу. Відрив промислово розвинених країн в області технологій та інфраструктурі від країн «периферії» постійно збільшується.

У сучасному секулярному суспільстві при відсутності усталеної системи цінностей, обумовленої традиційним культурним світоглядом, формується безліч індивідуальних свідомостей, орієнтованих «на іншого», особистостей, які зливаються у глобальну свідомість. Причому можна сказати, що це глобальний пантеїзм, про який попереджав ще А. де Токвіль, зазначаючи схильність до нього народів, що стали на шлях демократизації політичного життя [6].

Американський соціолог П. Бергер виділяє світську європейську культуру й секулярну міжнародну субкультуру, яку становить інтелігенція з утворенням західного типу в області гуманітарних і суспільних наук. Саме ця секулярна субкультура є «провідником прогресивних вірувань і цінностей». Попри те, що ця верства відносно тонка, вона дуже впливова, оскільки саме вона управляє суспільними інститутами, що дають оцінку явищам навколишньої дійсності: освітньою системою, засобами масової комунікації, рішеннями вищих ешелонів політичної системи. Попит на індивідуальну та колективну безпеку стає мегатрендом сучасності. Сьогодні інформаційну безпеку можна розглядати на декількох рівнях і у декількох проявах, але суть залишається: інформація є небезпечною зброєю. Тому у рамках цього тренду дослідники аналізують доступ до персональних даних, технічних засобів обробки і передачі даних і насамперед обчислювальних систем, захисту особистої свободи і права на особистий інформаційний простір [4].

Також учені розглядають інформаційний тероризм як насильницький пропаган-

дистський вплив на психіку, який не залишає для людини можливостей для критичної оцінки одержуваної інформації. Крім використання офіційних засобів масової інформації, інформаційний тероризм спирається на поширення певного типу чуток. Вони посилюють ту атмосферу страху і жаху, яку створюють терористи [5]. Ще одним аспектом цього тренду є кібертероризм, який дослідники визначають як протиправну атаку на інформаційні ресурси, несанкціоноване проникнення у комп'ютерні системи або мережі, наслідком якого є загроза для життя і здоров'я людей або настання інших тяжких наслідків – порушення громадської безпеки, залякування населення, провокування військового конфлікту [4].

Наступними загрозами є інформаційні або кібератаки – як самостійні впливи і як складові гібридної чи інформаційної війни. Особливого значення набуває не лише технічна та технологічна складова такої комунікації, а й змістовна, яка є високотехнологічною як за формами та методами подачі, так і за рівнем її продуманості. Сьогодні дуже поширеним є створення фейків, які підривають систему регулювання інформацією (створення «шуму», який не дає можливості зрозуміти, де факти, а де вигадки). Але ще більш поширеним є формування інформаційних модулів, орієнтованих на врахування потреб і особливостей (ціннісних, ментальних) окремих цільових груп. Тому сьогодні мова йде про смислові війни та інструменти м'якої сили. Ще одним проявом «сили слова» є меметична зброя (memetic warfare). Мем (з грец. – наслідувати) – одиниця культурної інформації, яка передається від людини до людини в інформаційному просторі. Це інформаційний вірус, що впливає на сприйняття дійсності, спонукає до дій та здатний до самовідтворення і розповсюдження. «Мем» розглядається як специфічний вірусний елемент, причиною виникнення якого є комерціалізація всіх сфер суспільного життя, розвиток мережевої комунікації, поява інтернет-спільнот як віртуальних соціумів [2].

Приклад мемів у бізнесі – вірусна реклама або ролики. Їхня мета – привернути увагу аудиторії до певного продукту. Меми сконструйовані так, щоб люди підсвідомо повторювали мелодії з рекламних роликів або виразно запам'ятовували образи. Меми розповсюджуються, як правило, у соціальних мережах та інтернет середовищі. Їхнє завдання – стереотипізація та спрощення інформації, «допомога» у розумінні складних процесів, нав'язування необхідних ідей, які зі свого боку змінюють поведінку людини. Приклади політичних мемів: хунта, майдауни, гейропа, потяг дружби, даунбас, ватник, а що там у хохлов, проФФесор, розіп'ятий хлопчик, кримнаш тощо [7].

Меми стають зброєю в інформаційній війні, за допомогою якої можна маніпулювати свідомістю та впливати на поведінку людини (Дуглас Рашкофф (Douglas Rushkoff) «Медіа вірус. Таємні послання в популярній культурі» (1995), «Стратегія результату» (2003); Річард Броуді (Richard Reeves Brodie) «Психічні віруси. Нова наука про меми» (1996)).

Інформаційна свідомість як складова компонента ідеології інформаційного суспільства у соціальній філософії ще не проаналізована. Попередніми результатами досліджень світових учених створено концептуальну парадигму інформаційної свідомості, її структуру та механізми відображення інформаційного соціуму, виражених художніми, естетичними, філософськими, політичними, метафізичними, онтологічними, правовими, релігійними поглядами [3].

Доктор Джо Діспенза (Joe Dispenza) став одним з перших, хто почав досліджувати вплив свідомості на реальність з наукової точки зору. Його теорія взаємозв'язку між матерією і свідомістю принесла йому світову популярність після виходу документального фільму «Ми знаємо, що робить сигнал». Ключове відкриття, зроблене Джо Діспензой, полягає у тому, що мозок не відрізняє фізичні переживання від душевних. Грубо кажучи, клітини «сірої речовини» абсолютно не відрізняють реальне, тобто матеріальне, від уявного, тобто від думок! Тільки вдумайтеся: наш характер, наші звички, наша особистість є всього лише набором стійких нейромереж, які ми у будь-який момент можемо ослабити або зміцнити завдяки усвідомленому сприйняттю дійсності! Концентруючи увагу усвідомлено і вибірково на те, чого ми хочемо досягти, ми створюємо нові нейронні мережі і можемо їх завдяки технологіям програмувати [5].

Україна вживає рішучих заходів на напрямі протидії сьогоденним загрозам і формування національної системи кібернетичної безпеки. Зокрема, у жовтні 2017 року підписано Закон України «Про основні засади забезпечення кібербезпеки України», яким визначені об'єкти кібербезпеки, кіберзахисту та критичної інфраструктури, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також повноваження суб'єктів їх забезпечення та засади координації їх діяльності. У січні 2018 року на базі СБУ спільно з НАТО відкрито перший Ситуаційний центр забезпечення кібербезпеки, ключовими можливостями якого є запобігання кібератакам, встановлення їх походження та формування пропозицій із протидії їм.

У лютому цього року Державною службою спеціального зв'язку та захисту інформації відкрито Центр реагування на кіберзагрози, який порівнюють із першою лінією оборони держави від кіберагресій. Водночас шляхи реалізації нових законодавчих норм потребують подальшого наукового вивчення [8, с. 34]. Останні кризові події доводять, що інформаційна безпека набуває визначальну роль у воєнній сфері. Безпосередньо у військовій справі рівень інформаційного потенціалу все більшою мірою обумовлює оперативність та ефективність прийняття рішень, структуру і якість озброєнь, оцінку рівня їх достатності та взагалі – результат збройного протистояння. Доктрина інформаційної безпеки України зазначає, що вагомою загрозою національним інтересам та національній безпеці України в інформаційній сфері є здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні [8, с. 23].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Основними напрями державної політики щодо забезпечення інформаційної безпеки зазначає забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади та ін. [1, с. 234]. Безумовно, генеза та новації законодавства у секторі інформаційної безпеки потребують детального, комплексного розгляду з погляду перспектив їх ефективної реалізації та можливих наслідків, що має слугувати предметом окремого дослідження та постійного моніторингу. Але у межах тез конференції уявляється не можливим надати повний обсяг проблемі, тому ми маємо намір зупинитися на окремих спільних недоліках законодавчих актів, процесу організаційно-правового забезпечення інформаційної безпеки у країні з акцентом на технологічно-правову складову окремих передбачених законодавцем заходів по їх реалізації. При подальшому удосконалюванні державної системи інформаційної безпеки України необхідно зберігати баланс між демократією і безпекою і не допускати створення одноособового органу державної влади, що здійснює діяльність у сфері інформаційної безпеки, варто дотримуватися колективних основ, тобто зміцнювати систему всіх державних органів, покликаних вирішувати проблеми інформаційної безпеки, ні в якому разі не допускати монополізму одного з них [6].

Висновки. Україна повинна брати активну участь у розробці і прийнятті міжнародних домовленостей, спрямованих на розвиток системи міжнародної взаємодії органів державної влади, що здійснюють діяльність у сфері інформаційної безпеки, зокрема по запобіганню і припиненню правопорушень у світовому інформаційному просторі. Розглянути можливість проведення консультацій з галузевими асоціаціями щодо формування платформ державно-приватного партнерства у сфері кібербезпеки. Розглянути можливість покладання на такі платформи обов'язку проведення огляду стану кібербезпеки у певній галузі на базі єдиної методологічної основи (там, де це можливо), що надалі могли б стати основою формування загальнонаціонального огляду з кібербезпекової тематики. З огляду на те, що значна кількість об'єктів критичної інфраструктури не лише знаходяться у власності приватних суб'єктів, але порушення їх роботи може вплинути на життєдіяльність навколишніх територій (які є зоною відповідальності та уваги місцевих органів державної влади органів місцевого самоврядування), доречним є розширення кола учасників державно-приватного партнерства, включаючи в його структуру регіональну та місцеву владу, а також структури цивільного захисту населення.

Електронна освіта демократизує і підриває традиційну систему освіти. Розвиток ресурсів електронної освіти надає багато можливостей, робить освіту більш доступною, вона втрачає віковий ценз.

Межі недоторканності приватного життя і захисту даних будуть переглянуті. Збереження великої кількості політичних та економічних даних буде сприяти розвитку профільних фахівців, появі нових спеціальностей на IT-ринку. Водночас можуть виникнути серйозні наслідки щодо недоторканності приват-

ного життя і кримінальних злочинів з використанням ІТ-технологій.

Гіперпов'язані спільноти, що самоорганізуються, будуть продукувати нові соціальні ініціативи, у них буде більше можливостей для колективних дій, петицій та відстоювання своїх прав. При цьому відкриті урядові ініціативи і доступ до суспільних даних призведуть до більшої прозорості і до орієнтації державних послуг на своїх громадян.

Стрімке поширення гіперпов'язаних мобільних пристроїв, мережевих сенсорів в обладнанні і інфраструктурі, 3D-технологій друку і перекладу з іноземних мов змінять глобальну інформаційну економіку. ІТ-технології – форма організації суспільства, де внаслідок широкого застосування інформаційно-комунікаційних систем, громадські організації, залучаються до прийняття державних рішень і участі у державному управлінні. Усім важливо зрозуміти, що штучний інтелект, сингулярність – не фантастика, а лише тільки тимчасове відставання. Виживання людей завжди залежало від суспільства, а зараз майбутнього інформаційного суспільства держави. Ми знаходимось на початку самої швидкої урбанізації людства, нанотехнологічного буму, кіборгізації нейроінтерфейсів, симбіозу біологічного та цифрового інтелекту, тому важливе сьогоднішнє визначення тенденцій розвитку інформаційно-комунікативних технологій як важливого сегменту управління державою.

ЛІТЕРАТУРА:

1. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. 408 с. С. 234.

2. Броді Р. Психічні віруси нова наука про меми. URL: https://scisne.net/a-443. – Назва з екрана.

3. Всесвітній економічний форум (World Economic Forum). URL: https://www.weforum.org/events/world-economic-forum-annual-meeting-2018. – Назва з екрана.

4. «Глобальний звіт про розвиток інформаційних технологій – 2016» (The Global Information Technology Report). URL: http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf. – Назва з екрана.

5. Діспенза Джо. Наша свідомість впливає на реальність. URL: http://samorozvytok.info/content/dzho-dispenza-nasha-svidomist-vplyvaye-na-realnist – Назва з екрана.

6. Дмитренко М.А. Проблемні питання інформаційної безпеки України. URL: journals.iir.kiev.ua/index.php/pol_n/article/download/3318/2997. – Назва з екрана.

7. Марутян Р. Інформаційні тренди сучасного. URL: matrix-info.com/2017/03/13/rosiya-z-bojovykamy-otrymaly-prodovzhe/ – Назва з екрана.

8. Поляков Ю. Информационная безопасность и средства массовой информации. М.: ИМПЭ им. А.С. Грибоедова, 2004. 67 с. С. 34.