УДК 342.31:321.011

РАДУТНИЙ О.Е., *доктор філософії (Ph.D.) з юридичних наук, доцент*,
доцент кафедри кримінального права № 1
Національного юридичного університету ім. Ярослава Мудрого

ІЛЮЗІЯ ТА РЕАЛЬНІСТЬ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ

Анотація: *В статті здійснено спробу продовження дискусії щодо змісту та обсягу поняття інформаційного суверенітету, його співвідношення з суверенітетом держави, фактичного стану інформаційного суверенітету окремих держав, в тому числі України, перспектив та тенденцій еволюції інформаційних відносин, в тому числі з огляду на досягнення науково-технічного прогресу (штучний інтелект, Інтернет, Всеосяжний Інтернет, криптовалюта, квантовий комп'ютер, Big Data, блокчейн тощо). Доведено тезу про те, що обов'язок захисту інформаційного суверенітету покладається не тільки на державу, але й на весь народ, окремою самостійною одиницею якого виступає кожний громадянин. Запропоновано рекомендації щодо захисту інформаційного суверенітету для держав, які не є технологічними або економічними лідерами сучасності.*

Ключові слова: *суверенітет, інформаційний суверенітет, національна безпека, штучний інтелект, криптовалюта, блокчейн, Big Data, інформація, інформаційний простір, Всеосяжний Інтернет, квантовий комп'ютер.*

Summary: *The article continues the discussion about the concept of information sovereignty, its relationship with the sovereignty of the state, the actual state of information sovereignty of individual states, including Ukraine, prospects and trends in information relations, including scientific and technological progress (artificial intelligence, Internet, Internet of Everythings, cryptocurrency, quantum computer, Big Data, blockchain etc.). It is proved that the duty to protect information sovereignty rests not only on the state, but also on the whole nation, a separate independent unit of which is each citizen. Recommendations for the protection of information sovereignty are made for states that are not technological or economic leaders of modernity.*

Keywords: *sovereignty, information sovereignty, national security, artificial intelligence, cryptocurrency, blockchain, Big Data, information, information space, Internet of Everythings, quantum computer.*

Аннотация: *В статье предпринята попытка продолжения дискуссии относительно содержания и объема понятия информационного суверенитета, его соотношения с суверенитетом государства, фактического состояния информационного суверенитета отдельных государств, в том числе Украины, перспектив и тенденций эволюции информационных отношений, в том числе с учетом достижений научно-технического прогресса (искусственный интеллект, Интернет, Всеобъемлющий Интернет, криптовалюта, квантовый компьютер, Big Data, блокчейн т.д.). Доказан тезис о том, что обязанность защиты информационного суверенитета возлагается не только на государство, но и на весь народ, отдельной самостоятельной единицей которого выступает каждый гражданин. Предложено рекомендации по защите информационного суверенитета для государств, которые не являются технологическими или экономическими лидерами современности.*

Ключевые слова: *суверенитет, информационный суверенитет, национальная безопасность, искусственный интеллект, криптовалюта, блокчейн, Big Data, информация, информационное пространство, Всеобъемлющий Интернет, квантовый компьютер.*

Постановка проблеми. За Жаном Боденом (фр. Jean Bodin), якого визнають автором поняття "суверенітет" [9, с. 60], останній полягає у незалежній та абсолютній

владі держави щодо створення і впровадження законів, забезпечення їх виконання силою свого примусу. Суверенітет є однією з ознак суверенної держави, він надає можливість самостійно здійснювати через відповідні державні структури функції стосовно формування і реалізації як внутрішньої, так і зовнішньої політики України, із суверенності України випливає її незалежність, незалежною може бути суверенна держава, яка має право самостійно вирішувати свої внутрішні й зовнішні справи без втручання будь-якої іншої держави [17, с. 84-85].

Разом з тим, спроби відшукати невід'ємний взаємозв'язок між суверенітетом та дотриманням прав людини і громадянина слід визнати лише даниною політичній моді, адже суверенною може бути не тільки демократична, але й тоталітарна держава, чому є численні приклади. Відстоювання інформаційного суверенітету може мати прояв у цензурі та(або) глушінні ворожих "голосів", як у в період існування СРСР, певних обмеженнях у користуванні Інтернетом, як це зараз має місце в деяких країнах, зокрема, Китаї (система фільтрації трафіку "Великий китайський фаервол"[1], ідентифікація кожного автора контенту через реєстрацію у Міністерстві промисловості та інформаційних технологій, обов'язкове для встановлення на кожний комп'ютер програмне забезпечення Green Dam для блокування пошуку забороненої або небажаної інформації тощо).

У своєму баченні ідеалу суверен претендує на повний контроль. Між тим, реальний суверенітет кожної держави суттєво поступається своїми якісними характеристиками теоретично омріяному зразку, якому протидіють численні фактори, зокрема, принципи пріоритетності світової демократії, прав і свобод людини, економічної свободи тощо. Оскільки реальний суверенітет національних держав поступово, але неухильно слабне, висловлюються припущення [10, с. 268-273] про їх зникнення з міжнародної арени у недалекому майбутньому під тиском глобалізаційних процесів [36].

Похідним від поняття "суверенітет" виступає термін "інформаційний суверенітет" (або, як синонім – "державний суверенітет в інформаційній сфері"), нормативне визначення якого закріплено в ст. 1 Закону України "Про Національну програму інформатизації" від 04.02.98 р. № 74/98-ВР [28] (хоча сам закон вказане поняття надалі не використовує, крім глосарію на початку) – здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави.

Проти використання поняття "інформаційний суверенітет" висловлюються слушні аргументи. Так, у 1996 р. відомий кіберлібертаріанець Дж. Барлоу (John Perry Barlow) проголосив у "Декларації незалежності кіберпростору" ("A Declaration of the Independence of Cyberspace"), що кіберпростір знаходиться поза суверенітетом і кордонами будь-якої держави [1]. У свою чергу, Б.А. Кормич формулює доречні питання про те, чи існує чітко визначений інформаційний кордон, що відокремлює інформаційну територію однієї держави від іншої, чи встановлює держава відповідні бар'єри на шляху інформації [18, с. 72], чи не вступає формулювання окремого "інформаційного" суверенітету у конфлікт з положеннями міжнародно-правових актів, зокрема Міжнародного пакту про громадянські й політичні права, якими встановлюються принципи свободи слова та інформації незалежно від кордонів [19, с. 15-16]. На таку саме засторогу відносно правової регламентації поняття

[1] Фаервол (англ. *firewall* – "вогняна стіна") – мережевий екран, або брандмауер (використано гру слів Great Firewall of China від Great Wall of China – Велика Китайська стіна).

“інформаційний суверенітет” вказує й О.М. Солодка, на думку якої воно за певних умов здатне порушити принцип транскордонності права доступу до інформації, яке в інформаційному суспільстві є одним із фундаментальних прав людини і громадянина та включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів (Загальна декларація з прав людини, Міжнародний пакт про громадянські та політичні права, Європейська конвенція про захист прав людини та основоположних свобод тощо) [35, с. 26-34]. Згідно з позицією О.В. Олійника цього є цілком достатньо, щоб відмовитися від спроб винайти окремий “інформаційний” різновид суверенітету [23, с. 54-59].

Контраргументи такій позиції можуть полягати у площині технічної можливості встановити перешкоди для вільного доступу інформації ззовні та забезпечити тотальний інформаційний контроль всередині (Північна Корея, Китай, РФ тощо) саме у межах географічної території, але не тільки. Крім того, інформаційний суверенітет не слід розглядати в якості явища, яке повністю відокремлене від інших суверенних аспектів правового феномену держави. Тож, інформаційний суверенітет є невід’ємною складовою загального суверенітету. Його виокремлення та самостійне дослідження обумовлене складністю розглядуваної системи та необхідністю більш детального аналізу її елементів. Крім того, загальний суверенітет не є посяганням на основні права та свободи людини та громадянина, принаймні, з цього приводу жоден дослідник ще не висловився.

Тож, відповідно до “Талліннського посібника із застосування міжнародного права до кібервійн” [8] діюче міжнародне право, яке засноване саме на територіальному принципі, може бути застосоване і до кіберпростору, таким чином держава володіє суверенітетом і юрисдикцією над всією інфраструктурою, яка знаходиться на її території.

На думку Н.А. Новікової [22], яку підтримує та розвиває О.М. Солодка [35, с. 26-34], повна відмова від окреслення меж інформаційного простору держави та інформаційного суверенітету суттєво обмежить вплив держави на відносини в інформаційній сфері та, оскільки поняття суверенітету включає в себе не лише здатність впливати на внутрішні процеси, але також місце держави серед країн міжнародної спільноти, може призвести до порушень у сфері інформаційної безпеки. Тож при формулюванні поняття, обсягу та ознак інформаційного суверенітету необхідно досягати певного балансу між правом на інформацію, свободою слова та інформації, з одного боку, та вимогами щодо державної інформаційної безпеки, з іншого.

Таким чином, реалізуючи свій інформаційний суверенітет, держава, перш за все, встановлює певні правила доступу, обігу та користування окремою інформацією, яка у визначений законодавством спосіб виокремлюється в якості державної, лікарської, комерційної або банківської таємниці, таємниці сповіді або усиновлення (удочеріння), службової інформації або іншої інформації з обмеженим доступом (ст.ст. 20, 21 Закону України “Про інформацію” від 02.10.92 р. № 2657-XII [27]). При цьому основними напрямами державної інформаційної політики є: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб’єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню

України до світового інформаційного простору (ст. 3 Закону України "Про інформацію" від 02.10.92 р. № 2657-XII [27]).

Результати аналізу наукових публікацій. Вагомі внески у дослідження проблем інформаційної безпеки та інформаційного суверенітету внесли як вітчизняні вчені, зокрема, О.А. Баранов, К.І. Бєляков, В.М. Брижко, В.І. Гурковський, О.Д. Довгань, О.П. Дзьобань, М.В. Карчевський, Б.А. Кормич, Н.А. Новікова, О.В. Олійник, В.А. Мисливий, В.А. Ліпкан, Ю.П. Лісовська, В.Г. Пилипчук, Н.А. Савінова, О.М. Солодка, О.В. Соснін, В.М. Супрун, Л.Є. Шиманський, авторський колектив (О.С. Онищенко, В.М. Горовий, В.І. Попик та інші) монографії "Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій" [21], автори (О.В. Задерейко, О.В. Троянський, Р.І. Чанишев) монографії "Концептуальні основи захисту інформаційного суверенітету України" [14] тощо, так і зарубіжні політичні та публічні діячі, письменники і науковці, в тому числі В. Гонг (Wenxiang Gong), Г. Кіссінджер (Henry Alfred Kissinger), З. Бжезінський (Zbigniew Kazimierz Brzeziński), І. Маск (Elon Musk), Р. МакЧесни (R.W. McChesney), Р. Кало (Ryan Calo), П. Асаро (Peter M. Asaro) та інші. Але тематика інформаційного суверенітету та пов'язаної з ним інформаційної безпеки залишається актуальною і потребує подальших досліджень.

Метою статті є визначення та аргументування змісту та обсягу поняття інформаційного суверенітету.

Завданням статті є продовження дискусії щодо змісту та обсягу поняття інформаційного суверенітету, його співвідношення з суверенітетом держави, фактичного стану інформаційного суверенітету окремих держав, в тому числі України, перспектив та тенденцій еволюції інформаційних відносин, в тому числі з огляду на досягнення науково-технічного прогресу (штучний інтелект, Інтернет, Всеосяжний Інтернет, криптовалюта, квантовий комп'ютер, Big Data, блокчейн тощо).

Основний виклад матеріалу. Одну з перших згадок про інформаційний суверенітет та тезу про необхідність його утвердження можливо відшукати у постанові КМ України "Про діяльність Кабінету Міністрів України, інших органів державної влади щодо забезпечення свободи слова, задоволення інформаційних потреб суспільства та розвитку інформаційної сфери в Україні" від 16.02.99 р. № 430-XIV [25].

Програмою діяльності Кабінету Міністрів України [31] до ключових завдань уряду віднесено розвиток і вдосконалення системи гарантування інформаційного суверенітету та інформаційної безпеки держави, запобігання злочинам у сфері інформаційних технологій. Відповідно до Доктрини інформаційної безпеки України (затв. Указом Президента України від 08.07.09 р. № 514/2009 [13], втратила чинність на підставі Указу Президента України від 06.06.14 р. № 504/2014 [26]) її основною метою було визначено створення в Україні розвиненого національного інформаційного простору і захист інформаційного суверенітету.

Положеннями попередньої редакції Закону України "Про інформацію" від 02.10.92 р. № 2657-XII (ст.ст. 53, 54) було передбачено [27], що основою інформаційного суверенітету України є національні інформаційні ресурси, в тому числі вся належна Україні інформація, незалежно від змісту, форм, часу і місця створення, Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами. Подальшими змінами вказані ст.ст. 53, 54 були виключені.

Втім, навіть з урахуванням обмеженої можливості належним чином охопити в окремому формулюванні всі суттєві ознаки певного явища, або відокремити його від інших (курйозний приклад: ДНК людини формально може бути визнано документом-

даними, адже на підставі ст. 1 Закону України "Про інформацію" від 02.10.92 р. № 2657-XII [27] вона є матеріальним носієм, що містить інформацію, зокрема, генетичну програму, основними функціями якого є її збереження та передавання у часі та просторі), слід зазначити, що нормативна дефініція "інформаційний суверенітет" (згідно з ст. 1 Закону України "Про Національну програму інформатизації" від 04.02.98 р. № 74/98-ВР [28]) є доволі недосконалою, оскільки залишає поза увагою здатність держави контролювати і регулювати (зрозуміло, що не повною мірою, не абсолютно, але лише у певних межах, що визначаються громадянським суспільством) потоки інформації всередині самої себе, у зв'язку з чим потребує подальшого вдосконалення.

Разом з тим, інший нормативний акт, зокрема, Закон України "Про науково-технічну інформацію" від 25.06.93 р. № 3322-XII [29], передбачає конкретні заходи забезпечення суверенітету України у чітко визначеній галузі, а саме у сфері науково-технічної інформації, в тому числі у вигляді: 1) організації та державної підтримки власних інформаційних систем і наданням для них можливостей шукати, фіксувати, отримувати, оброблювати і поширювати в інтересах суспільства науково-технічну інформацію, вироблену в Україні або в інших країнах світу; 2) встановлення власності держави на ресурси науково-технічної інформації, що формуються за рахунок коштів бюджету; 3) створення і розвитку національної системи науково-технічної інформації; 4) організації доступу інших держав до інформаційних ресурсів України на основі укладання угод та договорів про їх спільне використання, ліцензуванням і квотуванням науково-технічної інформації, яка може бути використана за межами України для виготовлення зброї, військової техніки, наукоємної продукції; 5) організації належної системи охорони та зберігання інформації.

Такі заходи можливо розповсюдити й на суміжні сфери діяльності, зокрема, передбачити у відповідному нормативному акті (не є принциповим, чи буде це Закон України "Про інформацію", "Про науково-технічну інформацію" або інший) можливість: 1) організації та державної підтримки національно-орієнтованих інформаційних систем (така підтримка має бути не лише зафіксована на папері, але проявлятися у конкретних формах податкових послаблень для існуючих організаційно-правових форм або нових стартапів[2], дешеві або безкоштовні державні кредити тощо); 2) встановлення чітких меж компетенції держави в інформаційній сфері (в тому числі, заборона втручання в інтимні (приватні) сфери життя людини, як-то регламентація природного або неприродного способу сексуальних відносин між двома фізичними особами, які мають статеву свободу та надали одна одній недвозначну згоду, такий рудимент попри усунення з інших статей залишився в чинній редакції ст.155 КК України); 3) встановлення власності держави на обладнання, лінії зв'язку та інформаційні ресурси, що формуються за рахунок коштів бюджету; 4) створення і розвиток національної системи інформаційних ресурсів; 5) організація доступу інших держав або самостійних суб'єктів до інформаційних ресурсів України з забезпеченням відповідного контролю; 6) організація належної системи охорони та зберігання

[2] Стартап (англ. *startup*), або стартап-компанія – щойно створена компанія, що будує свою діяльність на основі інновацій або інноваційних технологій, тільки вийшла на ринок або почала на нього виходити і володіє обмеженими ресурсами. Вперше термін "стартап" почали використовувати видання "Forbes" у серпні 1976 р. і "Business Week" у вересні 1977 р. для позначення компаній з короткою історією діяльності.

інформації на основі технології блокчейну[3] за відсутності єдиного уразливого ядра, що є майже гарантовано безпечним до появи квантового комп'ютеру[4] тощо.

Відповідно до положень ст. 17 Конституції України [16] захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки (ст.ст. 3, 19 Закону України "Про національну безпеку України" від 21.06.18 р. № 2469-VIII [30]) та національної системи кібербезпеки як складової системи забезпечення національної безпеки України (Стратегія кібербезпеки України, затв. Указом Президента України від 15.03.16 р. № 96/2016 [39]) є найважливішими функціями держави, справою всього Українського народу. Адже інформаційний простір є такою самою ареною протистояння, як і всі інші.

Інші положення Конституції України (зокрема, ст. 1 – "Україна є суверенна і незалежна, демократична, соціальна, правова держава", ст. 2 – "суверенітет України поширюється на всю її територію", ст. 5 – "носієм суверенітету і єдиним джерелом влади в Україні є народ" тощо) [16] надають підстави для висновку, що інформаційний суверенітет поширюється на всю її територію, а його носієм є народ. Але проголошенням інформаційного суверенітету справа далеко не завершується, адже його забезпечення та підтримання потребує значних зусиль.

Вбачається доцільним звернути увагу на той факт, що обов'язок захисту інформаційного суверенітету покладається не тільки на державу, але й на весь народ, окремою самостійною одиницею якого є кожний громадянин, кожна особистість, яка має правовий зв'язок з певним політико-територіальним утворенням як формою організації спільноти під управлінням уряду. Тож, з метою підтримання інформаційного суверенітету і, врешті решт, власної безпеки, на кожного окремого громадянина покладається обов'язок: 1) додавати зусиль для підвищення власної медіа-грамотності та медіа-освіти як сфери відповідальності за ту інформацію, яка допускається у свій особистий інформаційний простір; 2) перевіряти інформацію у декількох альтернативних джерелах, сортувати її за достовірністю (підтверджена, сумнівна) та оперативністю (історія питання, стан на сьогодні, прогноз); 3) вміти працювати з "інформаційним шумом" – непотрібною, надлишковою, зайвою або невчасною інформацією, яка заважає сприймати іншу і є набагато ефективнішою, ніж цензура, відрізняти його ненавмисні різновиди (фактичні помилки, механічні, технічні, коректорські тощо) та навмисні (політична пропаганда, PR-акції, маніпулятивні технології, комерціалізація тощо); 4) виховувати повагу до себе та країни, впевненість у собі; 5) відповідально ставитися до поширення інформації власними зусиллями;

[3] Блокчейн (ланцюжок блоків транзакцій, *blockchain,* або *block chai* від *block* – блок, *chain* – ланцюг) є розподіленою базою даних, яка зберігає захищений впорядкований ланцюжок записів (блоків), що містить часову позначку, хеш попереднього блока та дані транзакцій, подані як хеш-дерево [4]. У 2016 р. Міжнародною організацією зі стандартизації (ISO) було створено комітет для напрацювання міжнародного стандарту з технологій блокчейн.

[4] Квантовий комп'ютер – фізичний обчислювальний пристрій, функціонування якого ґрунтується на принципах квантової механіки, зокрема, принципі суперпозиції та явищі квантової заплутаності. Такий пристрій відрізняється від класичного комп'ютера тим, що останній оперує даними, закодованими у двійкових розрядах (бітах), кожен з яких завжди перебуває в одному з двох станів (0 або 1), у той час як квантовий комп'ютер використовує квантові біти (кубіти), які можуть знаходитися у суперпозиції станів. Інформатико-теоретичною моделлю такого обчислювального пристрою є квантова машина Тюрінга, або універсальний квантовий комп'ютер, який був розроблений Девідом Дойчем у 1985 р. [6].

6) критично мислити, мати незалежність у поглядах – що чим ширшим стає доступ до інформації, то більше з'являється нових способів її контролювати, відрізняти тональність подання інформації (надмірна емоційність, сенсаційність, претензія на оригінальність, вигляд корисності й документальності); 7) застосовувати контент-аналіз (переклад характеристик досліджуваних текстів у кількісні показники, які надалі статистично опрацьовуються) тощо.

О.В. Олійник, О.В. Соснін та Л.Є. Шиманський визначають інформаційний суверенітет України як виключне право України відповідно до Конституції і законодавства України та норм міжнародного права самостійно і незалежно, з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні і геополітичні національні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави [24].

Свідомо уникаючи посилання на державний суверенітет в якості опорного елемента для визначення інформаційного суверенітету, авторський колектив монографії "Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій" (О.С. Онищенко, В.М. Горовий, В.І. Попик, Ю.М. Половинчак, Л.А. Чуприна, О.В. Ворошилов та Т.Г. Кереза) [21, с. 13] пропонує визначення останнього, що згодом разом з усіма аргументами повторює О.Д. Довгань [12], як межі контролю інформаційних ресурсів, необхідних для існування і розвитку особи і суспільства, держави і нації, обумовлені специфікою їх призначення, характерними для них засобами досягнення суспільно значущих цілей, самобутністю і підтвердженою суспільною практикою традицією.

В.М. Супрун, в дослідженні "Теоретико-правові основи інформаційного суверенітету" [38], визначає поняття "інформаційний суверенітет" як стан самостійності формування певних ресурсів, даних, створених у результаті здійснення державою своєї свободи, за рахунок держави або суб'єктів держави, внаслідок реалізації права на інформацію, що забезпечує рівність її у міжнародному інформаційному просторі. Вказане надало досліднику підстави для висновку, що категорія "інформаційний суверенітет" є родовим поняттям по відношенню до категорії "інформаційна безпека", вони є взаємопов'язаними та взаємодіють між собою, оскільки реалізація засад інформаційного суверенітету здійснюється за допомогою прийомів та методів інформаційної безпеки.

Певною мірою дискутуючи з власною позицією (щодо раніше згаданої відмови від спроб винайти окремий "інформаційний" вид суверенітету), О.В. Олійник пропонує розглядати інформаційний суверенітет як суверенне право та відповідні функції, напрями державної діяльності в системі забезпечення державного суверенітету та безпеки розвитку соціальної системи, тому є цілком закономірним, що інформаційний суверенітет являє собою виключне право України відповідно до Конституції і законодавства України та норм міжнародного права самостійно і незалежно, з додержанням балансу інтересів особи, суспільства і держави визначати внутрішні і геополітичні інтереси у сфері інформаційної діяльності, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору (як центру, так і регіонів), створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку національним інтересам [23, с. 54-59].

Оскільки всі пропозиції щодо визначення розглядуваного явища мають право на існування, вбачається можливим запропонувати наступне, яке теж у подальшому може бути вдосконалене у якості доктринального: ***інформаційний суверенітет*** – *верховенство та незалежність держави в інформаційній сфері, її здатність визначати свою внутрішню та зовнішню інформаційну політику, створювати, контролювати і регулювати важливі потоки інформації на своїй території та у міжнародній взаємодії поза її межами, спроможність ефективно протидіяти зовнішнім та внутрішнім інформаційним викликам. Інформаційний суверенітет є одним з суттєвих показників самоідентифікації суспільства в умовах розвитку глобального інформаційного простору*.

Підґрунтям цього виступають політична та економічна незалежність окремої держави, контроль над технічними (апаратними) аспектами інформаційної взаємодії та програмним забезпеченням, каналами руху та центрами зберігання інформації (якщо вона не розпорошена за технологією блокчейн), дієвість методів і засобів створення, обробки та поширення певних відомостей тощо. Що більш незалежною є держава у використанні інформаційного простору (середовища, у якому обертаються інформаційні ресурси) та самих суверенних інформаційних ресурсів, то більшим рівнем інформаційного суверенітету вона володіє.

Інформаційний суверенітет не обмежений, але певним чином пов’язаний з територією держави та реальною географією, оскільки маршрути комунікації, сервери, сховища, перемикачі, з’єднувачі, технічні вузли та доменні зони мають конкретну локалізацію. Крім того, перехрещення потоків інформації від різноманітних навігаційних, мобільних та інших пристроїв утворюють мережу, яку можливо зіставити з певною територією.

Об’єктом інформаційного суверенітету виступають певні масиви інформації, в тому числі Big Data[5], в якості суверенних інформаційних ресурсів, та інформаційний простір. За Р.Р. Марутян, їх значення полягає у тому, що інформаційна основа діяльності в усіх сферах життя суспільства є фундаментом, або стратегічним ресурсом соціального розвитку й прогресу, за значущістю та специфічністю інформаційний ресурс перевищує всі інші [20, с. 493-497]. Суверенні інформаційні ресурси відображають особливості самобутності певної стійкої соціальної спільноти, є змістовною основою її соціальної інформаційної бази, відіграють роль орієнтиру та дороговказу подальшого самобутнього розвитку [21, с. 14-15].

Інформаційний суверенітет являє собою систему двох взаємопов’язаних компонентів, а саме технологічної та змістової складової. Кожна з них утворює більш складну підсистему взаємного впливу апаратних та програмних платформ, внутрішньої Інтернет-структури, засобів масової інформації, телебачення, пропаганди, ідеології, загальної технологічної грамотності тощо.

Факторами, які зсередини впливають на інформаційний суверенітет та формування інформаційного простору й інформаційних ресурсів є дійсний рівень демократичних відносин, рівень та структура інформаційного захисту від негативних впливів (інформаційна експансія або підривна діяльність, хакерські атаки тощо), наявність та чітке окреслення загального суспільного інтересу та об’єднання навколо нього, усвідомлення важливості й значення системи духовно-ціннісних орієнтирів,

[5] Великі дані (англ. *Big Data*) – феноменальне нагромадження даних та їх ускладнення, масиви інформації (як структурованої, так і неструктурованої) настільки великих розмірів, що традиційні способи та підходи їх обробки (здебільшого засновані на рішеннях класу бізнесової аналітики та системах управління базами даних) не можуть бути застосовані до них.

ефективність державного управління, поточний стан, обсяги фінансування, підтримки і розвитку сфери науки та освіти, відсталість або належний розвиток економічної та техніко-технологічної бази, наявність або відсутність доступу до попередніх пластів наукових напрацювань, які у друкованому вигляді розміщені по фондам, випередження або відставання правової бази забезпечення інформаційних відносин та інформаційного суверенітету тощо.

Чинниками впливу ззовні є глобальні тенденції розвитку інформаційного простору, вплив з боку лідерів міжнародної інформаційної взаємодії та інших суб'єктів міжнародних інформаційних відносин, в тому числі у вигляді можливості звертатися безпосередньо до населення поза національний уряд, порушення змістовної цілісності масивів інформації або їх організаційної структури тощо. Прикладною загрозою є контроль та несанкціонована обробка зашифрованих метаданих у якості цифрового сліду або "шпигунська" налаштованість програмних та апаратних засобів, що стало очевидним після викривальних заяв Е. Сноудена (Edward Joseph Snowden) з приводу масштабів діяльності Агенції національної безпеки США. Вбачається, що це лише надводна частина айсбергу тотального інформаційного контролю по всьому світу.

Окремою проблемою слід визнати проникнення чужої та(або) ворожої ідеології в суверенні й традиційні пласти інформації, зокрема світоглядної або релігійної, з несподіваними наслідками для певного суспільного укладу. Так, обряд каліцтва (мутиляції) жіночих статевих органів, що є поширеним переважно у африканських країнах, а також деяких регіонах Латинської Америки, Азії та Близького Сходу, але відповідно до Стамбульської конвенції (Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу з цими явищами - CETS № 210, Стамбул, 11 травня 2011 р. [15]) є нічим іншим, як гендерно зумовленим насильством та екстремальним проявом дискримінації, завдяки емігрантам стає значною проблемою для іншого світу, зокрема, у Великобританії, Німеччині, Італії, Канаді, США, Норвегії, Фінляндії, Франції, Чехії тощо, яким історично така практика не була притаманна. Вказаний виклик вимагає значних зусиль у просвітницькій роботі, а також передбачення кримінальної відповідальності (ст. 121 КК України).

Тим часом аргументи щодо доцільності впливу на інформаційний простір опонента, а так само його засоби і методи, вдосконалюються крізь віки ("Мистецтво війни" або "Закони війни учителя Суня" [37]). Тому в арміях і спеціальних службах багатьох країн засновуються та активно діють підрозділи для проведення операцій інформаційного впливу.

Ще однією системною проблемою для інформаційного суверенітету виступають досягнення науково-технічного прогресу. Так, за відсутність єдиного інформаційного ядра (серверу, сховища для зберігання тощо) певні відомості можуть виявитися поза досяжністю та контролем з боку держави, якщо вони розпорошені за технологією блокчейну. Крім того, завдяки Інтернету речей (Internet of Things, IoT, або краще – Всеосяжному Інтернету, Internet of Everythings, IoE) слабкі різновиди штучного інтелекту (Weak Artificial Intelligence, WAI, або Artificial Narrow Intelligence, ANI, або Applied Artificial Intelligence, AAI) можуть об'єднатися до рівня сильного (Strong Artificial Intelligence, SAI, або Artificial General Intelligence, AGI) або вищого ступеню суперінтелекта (Artificial Superintelligence, ASI) [33; 34] та утворювати певну загрозу своєю позаконтрольністю. Також сюди слід віднести: 1) вразливість технологій, які керують світом (системи енергопостачання, транспорт, фінансові ринки, алгоритмічне правосуддя, прикордонний контроль, військове забезпечення, надання медичної допомоги тощо) та мають численні недоліки (баги, помилки, дефекти), примітивні

паролі тощо; 2) незахищеність значної кількості пристроїв, які підключені до Всеосяжного Інтернету, детальну карту яких можливо згенерувати за допомогою пошукової системи Shodan за посиланням https://www.shodan.io; 3) недбало прописані комп'ютерні коди для більшості програм, що використовуються, зокрема, в роботі критичних інфраструктур, розробники таких програм більше звертають увагу на прибутковість, ніж на усунення вразливості; 4) загальна відсутність прозорості алгоритмів, що пояснюється необхідністю збереження комерційної, банківської, корпоративної, службової або державної таємниці та закріплюється на рівні нормативного акту або угоди користувача, яку ніхто не читає або не дочитує до кінця; 5) "чорна скринька" штучного інтелекту (наділеного властивостями щодо повної обізнаності у принципах своєї побудови і роботи, самонавчання, саморозвитку, самоперебудови та самовдосконалення, коли перша версія утворює вдосконалену версію самої себе і так переписує програму до нескінченності, а також не менш важливою функцією самостійності прийняття рішень та їх самостійного безпосереднього виконання), коли самі розробники вже не будуть впевнені у тому, що розуміються на всіх нюансах його роботи; 6) протиправне використання результатів поєднання біології з інформаційними технологіями, маніпуляція речовинами в атомному або молекулярному масштабі за допомогою нанотехнологій; 7) розроблення та використання персоналізованої інформаційної та(або) біологічної зброї, яка використовує унікальну біологічну, в тому числі генетичну, інформацію конкретної людини або певної людської групи; 8) ідентифікація думок (визначення об'єкту, про який думає людина) або навіювання думок за допомогою пристроїв на базі функціональної магнітно-резонансної томографії [7], управління та маніпулювання; 9) створення фактури (*від ред.*) дублікату особистості, зокрема, політичного діяча або державного посадовця вищого рангу, протиправне копіювання або повне перенесення (без залишків на первинному носієві) відомостей (*від ред.*) про свідомість, інтелект та особистість людини (самої себе або сторонньої особи) на цифровий або іншій носій [5]; 10) привласнення та(або) використання даних (*від ред.*) щодо чужої особистості на підставі підробки та(або) копіювання генетичних особливостей біологічного тіла та(або) інформаційної особистості шляхом опанування її цифрового сліду тощо.

Автор вважає за необхідне окремо підкреслити, що не є сучасним "луддитом" (англ. *luddites*, у трактуванні цього поняття як протиборства новітнім технологіям). Проте, прагнення до об'єктивності у доступних межах приводить до ще одного висновку: винахід та поширення криптовалюти (у її початковому розумінні, адже на сьогодні вже йдеться про можливість часткової централізації блокчейну) для держави є не просто потужним викликом. Дійсно, сучасні гроші перетворилися в інформацію у чистому вигляді. Через відсутність гарантій з боку держави вони мають назву фіатних (англ. *fiat currency*), або більш пом'якшено – фідуціарних грошей (від лат. *fiducia* – угода, договір, оснований на довірі). Фіатні гроші є типом валюти, цінність якої походить не від власної вартості або гарантії обміну на золото або іншу валюту, але від державного примусу та наказу (лат. *fiat* – "дозволяти", "нехай так буде!") використання саме їх як єдиного засобу платежу на території однієї або декількох країн.

Відповідно до принципу неподільності суверенітету держава одноосібно зосереджує всю його повноту і не поділяє його з будь-ким (втім, може делегувати окремі повноваження). Згідно з принципом єдності суверенітету у державі існує лише одна суверенна влада, яка, в тому числі визначає єдину на своїй території валюту. Втім, коли поєднуються разом декілька впливових чинників (загальна недовіра до держави та її інститутів, економічна криза тощо), то виникає соціальний запит на нові економічні

інструменти. Таким інструментом стала перша криптовалюта (цифрова грошова одиниця, для захисту якої застосовуються криптографічні методи) під назвою біткойн.

Важливим є питання про те, чи порушує криптовалюта фактом свого існування, розвитку та розповсюдження державний суверенітет, зокрема, України через зазіхання на окремі його ознаки, що закріплені у відповідній Декларації про державний суверенітет України від 16 липня 1990 р. [11], у тому числі: 1) верховенство (прерогативу влади) як відсутність іншої вищої суспільної влади на території країни; 2) самостійність як можливість одноособово приймати рішення усередині країни і ззовні за дотримання норм національного та міжнародного права; 3) повноту (універсальність) як поширення державної влади практично на всі сфери державного та суспільного життя (винятками з чого є відносини дружби, кохання тощо); 4) неподільність влади держави в межах її території, тобто одноособовість влади в цілому за можливість функціонального її поділу на законодавчу, виконавчу та судову гілки влади; 5) незалежність у зовнішніх та внутрішніх відносинах за дотримання норм міжнародного права та поважання суверенітету інших країн; 6) рівноправність у зовнішніх відносинах; 7) невідчужуваність, тобто неможливість довільної відчуженості легітимної та легальної влади тощо. *Неупередженою відповіддю може бути наступна*: так, порушує, зокрема самостійність (той, хто вводить у фактичний обіг незалежну від держави криптовалюту, перебирає на себе окремі економічні та політичні важелі останньої), повноту (система фактичного обігу криптовалюти є самокерованою та незалежною від держави), неподільність (поряд з державою з'являється новий потужний гравець, що є доволі несподіваним та загрозливим) тощо.

Звісно, криптовалюта не позиціонується в якості більш гарантованої, ніж фіатні гроші. За твердженням дійсної чи вигаданої особи на ім'я Сатоші Накамото (лист "Bitcoin: A Peer-to-Peer Electronic Cash System" ("Біткойн: однорангова система електронної готівки" [6]), криптовалюта може функціонувати лише за умови довіри.

Вагомими аргументами прихильності до криптовалюти є наступні: 1) децентралізована електронна довіра, яка забезпечується публічністю запису у ланцюжку блокчейну, що обумовлює неможливість підробити цей запис або протиправно його змінити, та наявністю у кожного біткойну своєї незмінної цифрової історії, що ускладнює можливість вчинення шахрайських дій; 2) криптографічний метод шифрування високої надійності (який невдовзі може зазнати поразки через появу квантового комп'ютера, який здатний стати центральним комп'ютером системи, через що буде знищено ідеологію блокчейну); 3) наявність копії єдиного журналу звітності у кожного користувача, створення можливості для забезпечення рівності всіх контрагентів, коли за допомогою використання технології блокчейн жоден з елементів системи не контролює базу даних електронних грошей у цілому, що унеможливлює контроль з боку сторонніх осіб та(або) протиправне втручання; 4) встановлення чітких правил, які виконуються автоматично; 5) саморегульованість та самокерованість системи, коли правила можуть бути відкоректовані лише за загальною згодою, а не на підставі рішення одного регулятора; 6) регулярність оновлення загального журналу звітності, що не потребує керування з єдиного центру або централізованого лічильника часу; 7) надання можливості звичайним учасникам прийняти фундаментальне рішення "чи приймаю цю криптовалюту у якості засобу платежу, або ні" (чого неможливо здійснити по відношенню до звичайних грошей). Але якщо, або як тільки криптовалюта стане грошима під контролем держави, виникне нова потреба у створенні пост-криптовалюти з новою ідеологією.

Якби всі або більшість впливових держав відреагували на появу криптовалют однаково негативно, узгоджено та у спосіб одностайної заборони, то у відповідних нормативних актах зарубіжних країн та КК України просто з'явилася би стаття під умовним номером 203-3 та умовною назвою "Дії з криптовалютою", аналогічно до того, як це свого часу несподівано мало місце щодо заняття гральним бізнесом (Закон України "Про внесення змін до деяких законодавчих актів України щодо удосконалення законодавства про заборону грального бізнесу в Україні" від 22.12.10 р. № 2852-VI [32]). Тоді право розвивалося би тільки у напрямку боротьби з будь-якою діяльністю, пов'язаною з криптовалютами. На цей напрямок з більшим або меншим успіхом витрачалися би державні кошти, створювалися нові підрозділи, окремі представники яких наживалися би на вічному протистоянні між бажанням та забороною, створювали би відповідні "дахи" над незаконною діяльністю, енергійно звітувалися тощо. Криптовалюту вдалося би остаточно знищити, якби відмовитися від використання електричної енергії та мережі Інтернет, але на це ніхто не пішов би.

Втім, історія повернула в інший "бік".

Окремі державні уряди виявилися настільки просякнуті ідеєю свободи та громадянського суспільства, що підтримали ідею криптовалют і взялися до її запровадження. З цього моменту точка неповернення була остаточно пройдена (сподіваємося, що так, але узгоджені світові карантинні заходи доводять можливість й протилежного). За таких умов кожний, хто надалі спробує забороняти криптовалюти або вести боротьбу з ними, залишиться на узбіччі економічного, науково-технічного та іншого розвитку. Але слід відзначити, що такий прогрес розмиває межі суверенітету, про що йшлося вище.

Між тим, повага до суверенітету, в тому числі інформаційного, є одним з основних принципів сучасного міжнародного права, які закріплені в Статуті ООН та інших міжнародних актах. В ідеалі всі держави мають бути рівноправними щодо власного інформаційного суверенітету, але реальність є дещо іншою. Формально незалежні, більшість країн світу зазнають відкритого або прихованого впливу з боку потужних інформаційних гігантів, якими є як окремі держави (США, Китай, РФ, Японія, Ізраїль тощо), так і транснаціональні корпорації (Apple, Amazon, Facebook, Google, Microsoft, IBM тощо), що мають статус технологічних флагманів, розуміються на сучасному обладнанні та програмному забезпеченні, Big Data, нейронних мережах, штучному інтелекті, хмарних обчисленнях тощо. Фактично це означає спроби маніпуляції місцевим населенням, політичними або економічними елітами, інколи відвертий диктат, інформаційну дискримінацію, неповагу до права вільно обирати й розвивати власну інформаційну систему, встановлювати власні правила суверенного інформаційного середовища тощо. У ряді випадків держава поступається своєю суверенністю на користь олігополії, що керує глобальними телекомунікаційними мережами, включаючи Інтернет та інформаційні соціальні майданчики.

Тож, фактичний рівень інформаційного суверенітету держави залежить від її реального розташування по відношенню до світового інформаційного ядра (у центрі якого знаходяться зазначені країни та корпорації), наближення або віддалення від якого може вказувати на зміцнення або ослаблення інформаційного суверенітету. До того ж фактичне набуття ознак інформаційного суверенітету кожною державою насправді не входить у сферу зацікавленості з боку інформаційного ядра, що викликає відповідний супротив та блокування зазначеного процесу.

Так само як і загальний суверенітет, інформаційний суверенітет зазнає впливу у вигляді "де-суверенізації", що пов'язано із зростанням ролі глобального управління,

спробами подолати загальний суверенітет як “останню барикаду” та базову одиницю Вестфальської системи міжнародних відносин [12, с. 102-112], обґрунтуванням ревізії суверенітету як “знизу”, так і “згори” [2], перерозподілом владних функцій від національно-державного рівня до міжнаціонального, інтеграційними процесами між державами з одночасною децентралізацією всередині їх тощо. Втім, протилежну точку зору з цього приводу висловлює С. Краснер (Stephen D. Krasner), на думку якого глобалізація не підриває фундаментальні основи суверенітету держав, адже вона є лише викликом ефективності державного контролю, але це не є свідченням того, що нові виклики суттєво відрізняються від старих [3], що може стосуватися й інформаційного суверенітету.

Таким чином, здатність проводити самостійну інформаційну стратегію є показником високого рівня суверенітету держави. Певний рівень інформаційного суверенітету корелює з здатністю держави до ефективного виконання своїх функцій, самостійного розв’язання внутрішніх проблем та протистояння зовнішнім викликам. Інформаційний суверенітет держави забезпечується високорозвиненою економічною, технологічною та військовою сферами, ефективністю політичної еліти, в тому числі здатністю оптимально управляти наявними ресурсами в поточних умовах.

Порушення інформаційного суверенітету виявляється в конкретних формах, зокрема, крім вищенаведених, це також можуть бути перешкоджання здійсненню виборчого права, фальсифікація виборчих документів, документів референдуму, підсумків голосування, заклики до дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, надання інформаційної допомоги іноземній державі, збирання з метою передачі або передача відомостей, що становлять державну, банківську, комерційну таємницю, відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, розголошення державної таємниці, порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер, посягання на здоров’я людей під приводом проповідування релігійних віровчень чи виконання релігійних обрядів, порушення таємниці листування, телефонних розмов, завідомо неправдиве повідомлення про загрозу безпеці громадян, публічні заклики до вчинення терористичного акту, незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації, умисне пошкодження ліній зв’язку тощо, відповідальність за вказані дії передбачена ст. ст. 109, 111, 114, 157, 159, 163, 170, 181, 231, 258-2, 259, 328, 330, 359, 360 КК України тощо. Способом посягання на інформаційний суверенітет можуть виступати окремі дії, відповідальність за які передбачена розділом XVI “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” Особливої частини КК України (ст.ст. 361 – 363-1) тощо.

Наведене породжує питання про те, що цьому може протиставити країна, яка не є технологічним або економічним лідером та віддалена від світового інформаційного ядра. По-перше, вона має не у гучних гаслах, але у конкретний спосіб підтримувати національну освіту та науку, вітчизняного виробника програмного забезпечення та технологічного обладнання, що має в перспективі зменшити монопольний вплив зарубіжних постачальників. По-друге, з метою усунення похибок людського фактору – постійне навчання та тренування, заохочення до саморозвитку, формулювання об’єднуючої національної ідеї, збереження й розвиток досвіду і традицій, як по горизонталі (створення нових інформаційних масивів), так і по вертикалі (передача

знань від одних поколінь до інших), популяризація зразків бажаної поведінки, позбавлення відчуття меншовартості у порівнянні з іншими країнами або спільнотами, які нещодавно були такі самі, якщо не гірше.

Висновки та пропозиції.

Інформаційний суверенітет існує та є складовою частиною загального суверенітету держави.

Інформаційний суверенітет *можливо визначити* як верховенство та незалежність держави в інформаційній сфері, її здатність визначати свою внутрішню та зовнішню інформаційну політику, створювати, контролювати і регулювати важливі потоки інформації на своїй території та у міжнародній взаємодії поза її межами, спроможність ефективно протидіяти зовнішнім та внутрішнім інформаційним викликам. Інформаційний суверенітет є одним з суттєвих показників самоідентифікації суспільства в умовах розвитку глобального інформаційного простору, він поширюється на всю її територію, але нею не обмежується, його носієм є народ. У зв'язку з цим обов'язок захисту інформаційного суверенітету покладається не тільки на державу, але й на весь народ, окремою самостійною одиницею якого виступає кожний громадянин.

Реальний суверенітет багатьох держав зазнає значного впливу, поступово слабне, через що висловлюються припущення про їх зникнення з міжнародної арени у недалекому майбутньому під тиском глобалізаційних процесів. Такого самого впливу зазнає й інформаційний суверенітет. Факторами, які впливають на нього зсередини є дійсний рівень демократичних відносин, рівень та структура інформаційного захисту від негативних впливів, наявність та чітке окреслення загального суспільного інтересу та об'єднання навколо нього, усвідомлення важливості й значення системи духовно-ціннісних орієнтирів, ефективність державного управління, поточний стан, обсяги фінансування, підтримки і розвитку сфери науки та освіти, техніко-технологічна база, наявність або відсутність доступу до попередніх пластів наукових напрацювань тощо. Чинниками впливу ззовні є глобальні тенденції розвитку, вплив з боку лідерів міжнародної інформаційної взаємодії, проникнення чужої хибної ідеології або поглядів у непідготовлене суспільство тощо.

Досягнення науково-технічного прогресу можливо використати як на благо, так і проти нього (за Парацельсом, все може бути як ліками, так і отрутою, те й інше визначає тільки доза та напрямок використання). Так, за відсутності єдиного інформаційного ядра (серверу, сховища для зберігання тощо) певні відомості можуть виявитися поза досяжністю та контролем з боку держави, якщо вони розпорошені за технологією блокчейну. Завдяки Всеосяжному Інтернету слабкі різновиди штучного інтелекту можуть об'єднатися до рівня сильний або суперінтелект та утворити певну загрозу своєю позаконтрольністю. Світом керують вразливі або непрозорі технології та недбало прописані комп'ютерні коди. Поява та поширення криптовалюти є потужним викликом для держави, адже посягає на самостійність (особа, яка вводить у фактичний обіг криптовалюту незалежно від держави, перебирає на себе економічні та політичні важелі останньої), повноту (система фактичного обігу криптовалюти є самокерованою та незалежною від держави), неподільність (поряд з державою з'являється новий потужний гравець, що є доволі несподіваним та загрозливим) тощо.

Держава, яка не є технологічним або економічним лідером, крім заходів щодо охорони суверенітету та національної безпеки, має не припиняти зусиль щодо захисту власного інформаційного суверенітету, у тому числі у конкретний спосіб підтримувати національну освіту та науку, вітчизняного виробника програмного забезпечення та технологічного обладнання, запровадити постійне навчання та тренування на рівні кожної

особи як найменшої одиниці суспільства та народу, дієво заохочувати до саморозвитку, сформулювати об'єднуючу національну ідею, здійснювати заходи щодо збереження та розвитку досвіду і традицій (як по горизонталі – створення нових інформаційних масивів, так і по вертикалі – передача знань від одних поколінь до інших як-то передбачено преамбулою Конституції України "усвідомлюючи відповідальність перед Богом, власною совістю, попередніми, нинішнім та прийдешніми поколіннями"), популяризувати зразки бажаної поведінки, підтримувати позбавлення відчуття меншовартості у порівнянні з іншими країнами або спільнотами, які нещодавно були такі самі тощо.

Перспективи подальших досліджень. Порушені питання та надана їм авторська оцінка є дискусійними та відкритими для конструктивної критики і широкого обговорення з огляду на їх актуальність та важливість для забезпечення подальшого розвитку інформаційного суспільства.

Використана література

1. Barlow J.P. A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence (дата звернення: 10.12.2020).

2. Hoffmann S. The Politics and Ethics of Military Intervention. *Survival.* 1996. Vol. 37:4. P. 29-51.

3. Krasner, Stephen D. Globalization, Power and Authority. The Evolution Of Political Knowledge: Democracy, Autonomy, And Conflict In Comparative And International Politics. *Ohio State University Press.* 2003. 430 p.

4. Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. *Princeton: Princeton University Press.* 1st Edition – July 19, 2016. 336 p.

5. Novella Steven. The Continuity Problem. Neuroscience. Apr 23, 2013. URL: https://theness.com/neurologicablog/index.php/the-continuity-problem (дата звернення: 10.12.2020).

6. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.* Nov 1. 2008. URL: https://bitcoin.org/bitcoin.pdf. – (Цитується за: Росс Алек. Індустрії майбутнього / пер. з англ. Наталія Кошманенко. Київ: Наш формат, 2017. 320 с. С. 116).

7. Stahl Lesley. How Technology May Soon "Read" Your Mind - Incredible Research Lets Scientists Get A Glimpse At Your Thoughts. *CBS News.* Dec. 31, 2008. URL: https://www.cbsnews.com/news/how-technology-may-soon-read-your-mind (дата звернення: 10.12.2020).

8. Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence / general editor Michael S. Schmitt. New York: Cambridge University Press, 2013. 302 p. P. 25, 71. URL: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (дата звернення: 10.12.2020).

9. Боден, Жан. Філософський енциклопедичний словник / В.І. Шинкарук (гол. редкол.) та ін. Київ: Інститут філософії імені Григорія Сковороди НАН України: Абрис, 2002. 742 с. С. 60.

10. Горбатенко В.П. Національна держава та її суверенність в умовах глобалізації / *Українсько-польські політологічні студії:* наук. зб. Вип. 3 / за ред. В. Горбатенка, І. Ставови-Кавки. Київ: Інститут держави і права ім. В.М. Корецького НАН України, 2013. С. 268-273.

11. Декларація про державний суверенітет України: Закон України від 16.07.90 р. *Відомості Верховної Ради УРСР (ВВР).* 1990. № 31. Ст. 429. URL: https://zakon.rada.gov.ua/laws/show/55-12#Text (дата звернення: 10.12.2020).

12. Довгань О.Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право.* № 3(12)/2014. С. 102-112.

13. Доктрина інформаційної безпеки України: Указ Президента України від 08.07.09 р. № 514/2009. URL: https://zakon.rada.gov.ua/laws/show/514/2009#Text (дата звернення: 10.12.2020).

14. Задерейко О.В. Троянський О.В., Чанишев Р.І. Концептуальні основи захисту інформаційного суверенітету України: монографія. Одеса: Фенікс, 2018. 112 с.

15. Про запобігання насильству стосовно жінок і домашньому насильству та боротьбу з цими явищами: Конвенція Ради Європи від 11 травня 2011 р. CETS № 210: офіційний переклад. URL: https://rm.coe.int/1680462546 (дата звернення: 10.12.2020).

16. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: https://zakon. rada. gov.ua/laws/show/254к/96-вр#Text (дата звернення: 10.12.2020).

17. Конституційне право України: підручник для студентів вищих навчальних закладів / за ред. академіка АПрН України, д.ю.н., проф. Ю.М. Тодики, д.ю. і політ. наук, проф. В.С. Журавського. Київ: Видавничий Дім "Ін Юре", 2002. 544 с. С.84- 85.

18. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посібн. Київ: Кондор, 2008. 382 с.

19. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. …д-ра юрид. наук: спец. 12.00.07. Харьков. 2004. С. 15-16.

20. Марутян Р.Р. Національні інформаційні ресурси як першооснова інформаційного суверенітету України: матеріали круглих столів та конф. *Актуальні проблеми міжнародної безпеки: український вибір*, проведених НІПМБ впродовж 2008 – 2009 років. – (Нац. ін-т проблем міжнар. безпеки). Київ: Стилос, 2010. С. 493-497.

21. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій / О.С. Онищенко, В.М. Горовий, В.І. Попик та ін. – (НАН України, Нац. б-ка України ім. В.І. Вернадського). Київ: НБУВ, 2011. 154 с.

22. Новікова Н.А. Інформаційний простір як основа інформаційної функції сучасної держави. *Актуальні проблеми держави і права*. 2011. С. 365-373. URL: http://www.apdp.in.ua /v61/50.pdf (дата звернення: 10.12.2020).

23. Олійник О.В. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки України. *Наукові записки Інституту законодавства Верховної Ради України*. 1/2015. С. 54-59.

24. Олійник О.В., Соснін О.В., Шиманський Л.Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. *Держава і право.* 2001. Вип. 13. С. 534-541. URL: http://www.niss. gov.ua/book/Sosnin_2.htm (дата звернення: 10.12.2020).

25. Про діяльність Кабінету Міністрів України, інших органів державної влади щодо забезпечення свободи слова, задоволення інформаційних потреб суспільства та розвитку інформаційної сфери в Україні: постанова КМ України від 16.02.99 р. № 430-XIV. *Відомості Верховної Ради України (ВВР*). 1999. № 16. Ст. 99.

26. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про скасування деяких рішень Ради національної безпеки і оборони України" та визнання такими, що втратили чинність, деяких указів Президента України: Указ Президента України від 06.06.14 р. № 504/2014. URL: https://zakon.rada.gov.ua/laws/show/n0008525-14#Text (дата звернення: 10.12.2020).

27. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. URL: https://zakon.rada. gov.ua/laws/show/2657-12#Text (дата звернення: 10.12.2020).

28. Про Національну програму інформатизації: Закон України від 04.02.98 р. № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text (дата звернення: 10.12.2020).

29. Про науково-технічну інформацію: Закон України від 25.06.93 р. № 3322-XII. URL: https://zakon.rada.gov.ua/laws/show/3322-12?find=1&text=сувер#w1_1 (дата звернення: 10.12.2020).

30. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 10.12.2020).

31. Програма діяльності Кабінету Міністрів України від 05.06.02 р. URL: https://zakon. rada.gov.ua/laws/show/n0002120-02/print1389943255155351#Text (дата звернення: 10.12.2020).

32. Про внесення змін до деяких законодавчих актів України щодо удосконалення законодавства про заборону грального бізнесу в Україні: Закон України від 22.12.10 р. № 2852-VI. *Відомості Верховної Ради України (ВВР).* 2011. № 28. Ст. 253. URL: https://zakon.rada. gov.ua/laws/show/2852-17#Text (дата звернення: 10.12.2020).

33. Радутний О. Суб'єктність штучного інтелекту у кримінальному праві. *Право України.* 1/2018. С. 123-136.

34. Радутний О.Е. Додаткові аргументи щодо правосуб'єктності штучного інтелекту: матеріали другої наук.-практ. конф. *Інтернет речей: проблеми правового регулювання та впровадження,* м. Київ, 29 лист. 2018 р. / упоряд. В.М. Фурашев, С.О. Дорогих. Київ: КПІ ім. Ігоря Сікорського, Вид-во "Політехніка". 2018. 168 с. С. 46-50.

35. Солодка О.М. Генеза наукових та правових підходів до формулювання концепту "інформаційний суверенітет". *Інформаційна безпека людини, суспільства, держави.* 2015. № 3(19). С. 26-34.

36. Смолянюк В.Ф. Десуверенізація сучасних держав як наслідок глобалізації. *Науково-інформаційний вісник Академії національної безпеки*. 2014. Вип. 1(1). С. 58-81. URL: http://nbuv.gov.ua/UJRN/nivanb_2014_1_6. (дата звернення: 10.12.2020).

37. Сунь-цзи. Мистецтво війни / пер. Лесняк С. Львів: Видавництво Старого Лева, 2015. 112 с.

38. Супрун В.М. Теоретико-правові основи інформаційного суверенітету: автореф. дис. ...канд. юрид. наук: 12.00.01. Харьків. 2010. 21 с.

39. Стратегія кібербезпеки України: Указ Президента України від 15.03.16 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016?find=1&text=безпек#Text (дата звернення: 10.12.2020).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~