НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕНЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Монографія

Харків 2019

УДК 351.86: 004.056

Монографію розглянуто та рекомендовано до друку Вченою Радою
Національного університету цивільного захисту України
Протокол № 9 від 23. 05..2019

Рецензенти:

Дегтяр А.О.. – д.держ.кпр., професор, заслужений діяч науки і техніки України, завідувач кафедри менеджменту і адміністрування Харківської державної академії культури.

Дацій О.І. – д.е.н., професор, заслужений працівник освіти України, зав.кафедри фінансів, банківської та страхової справи Межрегіональної академії управління персоналом м. Київ.

Державне регулювання забезпеченям інформаційної безпеки: Монографія / С.М. Домбровська, М.М. Удянський, Л.В. Домбровський, Н.М. Карпеко. НУЦЗУ.- 2019. – 279 с.

В монографії розглянуто питання дослідження і формування наукового базису інноваційних перетворень у вітчизняному публічному адмініструванні. Процес державного регулювання забезпечення інформаційної безпеки, що є одним із стратегічних ресурсів країни. У цьому аспекті розробка проблем державного регулювання формуванням та забезпеченням інформаційної безпеки є значним внеском у розвиток наукової теорії інноваційних перетворень в сучасному інформаційному середовищі. Теоретичні положення монографії можуть бути впроваджени в діяльність Національного університету цивільного захисту, Інституту державного управління у сфері цивільного захисту і використані в навчально-методичній роботі при вдосконаленні програмно-методичного забезпечення навчального процесу в системі підготовки магістрів та підвищення кваліфікації державних службовців.

С.М.Домбровська,
М.М. Удянський,
Л.В. Домбровський
Н.М. Карпеко
2019

ЗМІСТ

ВСТУП

В умовах соціально-економічних змін і перетворень в українському суспільстві, що відбуваються останні роки під натиском інформаційної експансії у всіх сферах життя в Україні і світі, дозволяє говорити про наближення до глобального інформаційного суспільства. При цьому, одночасно створюються можливості настання бажаних і загрозливих наслідків як для суспільства в цілому, так і для окремої людини. Сучасна людина в суспільстві, що прямує до інформаційного, занурена в світ технологій і надміру інформації. В кожній сфері життєдіяльності суспільства активно використовуються інформаційні технології (ІТ), що спричиняє посилення інформаційних впливів. Динамічний розвиток дійсності також вимагає перегляду підходів до розуміння безпеки суспільства, держави і, насамперед, людини. Сформоване наприкінці XX століття бачення державної безпеки, яке відштовхувалось від відсутності небезпеки або нейтралізації загроз, і було, насамперед, адаптоване до потреб держави, не спроможне відобразити сутність безпеки в сучасному глобалізованому і перенасиченому інформацією світі.

Перехід до нових стратегій використання публічної інформації в управлінні суспільством засвідчив, що сьогодні жодна держава не може претендувати на лідерство й конкурентоспроможність без ефективної інформаційної політики, опанування нових методів підтримки взаємодії владних структур з інститутами громадянського суспільства. Достовірність, надійність державної інформаційної політики, найефективніше використання інформаційних ресурсів, зовнішніх і внутрішніх інформаційних каналів підвищують якість державноуправлінських рішень, стабільність соціально-політичного розвитку країни. Отже, виважена інформаційна політика визначає успішність функціонування державної влади в цілому.

Наприкінці XX ст. інформаційно-правові дослідження були сконцентровані на вивченні особливостей суспільних відносин, що виникали у зв’язку з все більш активним використанням ІТ, і намаганням врегулювати

видозмінені відносини. При цьому, у світі склалось дві тенденції державого регулювання відносин у інформаційній сфері: використовувати за аналогією законодавство, що існує, при цьому створюючи нові норми лише щодо дійсностей, які повстають у зв'язку з всеосяжною інформатизацією; або творити нове законодавство. Водночас, врегулювання вже існуючих інформаційних відносин виявилось недостатнім, що підкреслило необхідність ефективної реалізації прогностичної функції забезпечення державної безпеки. Становлення законодавства не встигає за здобутками науковотехнічного прогресу, у зв'язку з чим виникають нові суспільні відносини, які, доволі часто, вимагають насамперед етичної, а вже потім державно-управлінської оцінки соціумом.

Дослідження реалій суспільства, що прямує до інформаційного, і умов безпечного існування людини в державі, свідчить про необхідність виявлення закономірностей та тенденцій виникнення та актуалізації інформаційних загроз, а також визначення меж необхідного і можливого втручання держави шляхом державного регулювання та впровадження державних форм інституціонального захисту.

Достовірність, надійність державної інформаційної політики, найефективніше використання інформаційних ресурсів, зовнішніх і внутрішніх інформаційних каналів підвищують якість державноуправлінських рішень, стабільність соціально-політичного розвитку країни. Отже, виважена інформаційна політика визначає успішність функціонування державної влади в цілому.

За оцінкою більшості зарубіжних та вітчизняних дослідників, наприкінці XX ст. відбулося якісне оновлення інформаційно-комунікаційних технологій, кардинально змінюючи політичну сферу, трансформуючи її інститути та норми, конструюючи нові моделі взаємодії влади та суспільства. Методологічні засади дослідження інформації, суспільства в концепціях постіндустріалізму та глобалізації засобів масової комунікації розглядалися у працях зарубіжних дослідників: Р. Арон, Д. Бела, П. Бурдьє , Н. Вінера, І. Валерстайна, А.

Герберта, П. Друкера, У. Дайзарда, Е. Гіденса, Дж. Гелбрейта , Дж. Гудбі, У. Ешбі , М. Кастельса , Й. Масуди, М. Маклюена , М. Масмоуди, М. Пората, Т. Розака, Т. Стоуньєра, Е. Тоффлера, К. Шенона й ін.

При проведенні дослідження державної інформаційної політики, використовувалися теоретичні та практичні доробки, які відображені у працях: І. Арістової, В. Бакуменка, А. Баровської, Я. Базилюка, О. Бодрука, І. Бінько , М. Бутка, Б. Гаєвського, О. Григора, О. Данільян, А. Дєгтяря, В. Дзюндзюка, Ю. Кальниша, В. Князєва, М. Корецького, О. Крюкова, М. Лесечка, О. Логінова, В. Лугового, О. Олійника, Г. Почепцова, Л. Полякової , П. Петровського, О. Радченка, М. Сендзюка, В. Токовенка, В. Цимбалюка, С. Чукут й ін. Важливість концептуального осмислення проблем формування та реалізації державної безпеки у сфері інформаційної політики диктується і необхідністю коригування тезауруса, пов'язаного з цим феноменом.

Для реалізації мети й завдань дослідження використовувався комплекс загальнонаукових методів. Методологічною основою дослідження є системний підхід, що дозволяє уявити державну інформаційну політику як складну структурно організовану систему, внутрішня побудова й елементна база якої потребують інтенсивного розвитку. Ядром методології дослідження є атрибутивно-онтологічний підхід, що припускає виявлення вихідних, базових, родових властивостей розвитку явища й поняття державної інформаційної політики. Застосування системно-аналітичного методу дозволило розглядати державну інформаційну політику як систему, що функціонує на основі не лише внутрішнього саморозвитку, але і під впливом зовнішніх факторів, та сформувати комплекс дослідних моделей, за допомогою яких можливі об'єктивний аналіз і осмислення сутності державної інформаційної політики, а також наукових принципів її формування.

Синтез системного, статистичного, синергетичного та інформаційного підходів дозволив визначити шляхи вдосконалення інформаційно-комунікаційної інфраструктури державноуправлінської діяльності та надав можливість запропонувати новий підхід до формування Концепції державної

інформаційної політики. Завдяки емпіричним методам дослідження, у результаті аналізу нормативних правових документів, виявлено недостатність, фрагментарність правової бази у сфері розвитку державної інформаційної політики та забезпечення інформаційної безпеки. На основі порівняльного аналізу доктринальних документів та нормативно-правових актів у галузі регулювання інформаційної сфери країни з'ясовано невідповідності концептуальних підходів та нормативно-правового регулювання інформаційних процесів і відносин між суб'єктами інформаційного простору.

Нормативну основу дослідження складає національне законодавство України і зарубіжних країн, а також міжнародно-правові акти. Емпіричною основою дослідження стали матеріали нормотворчої практики органів державної влади, політико-правова публіцистика, довідкові видання, статистичні матеріали.

Загальним результатом дослідження є обґрунтування концептуальних положень та практичних пропозицій щодо формування та розвитку дієвих механізмів державного регулювання розвитком інформаційної сфери для забезпечення державної безпеки України. Основні теоретичні положення, висновки та рекомендації о дослідження можуть бути реалізовані при формуванні та реалізації інформаційної політики органів державної влади, у визначенні статусу ідеології в умовах трансформації інформаційної сфери України та інших споріднених наукових галузях.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ НАУКОВИХ ДОСЛІДЖЕНЬ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СУСПІЛЬСТВІ

1.1. Суть та зміст державного регулювання інформаційною безпекою людини

Класичне визначення поняття «інформація» в його соціологічному аспекті доповнюється некласичним розумінням її соціально-економічної природи, що набуває під впливом глобалізаційних процесів якісно інших властивостей, стає ключовим при здобутті знань, формує уявлення про реалії соціальної дійсності й відтворює в цілому картину світу. Інформація має самостійну цінність, свої специфічні закономірності функціонування й розвитку, здатна до випереджального впливу на інформаційну політику, виступає безпосередньою причиною, що визначає вибір того або іншого варіанту політичного розвитку, поведінки різних соціальних груп і окремих громадян, переведення державної системи в новий стан. Інформація є вихідним ресурсом для розроблення інформаційної політики та здійснення державного управління в будь-якій сфері життєдіяльності суспільства й держави. Розвиток науки про безпеку в напрямку інформаційної безпеки суттєво залежить від занурення конкретного суспільства і держави в реальність інформаційного вибуху і формування інформаційного суспільства. Рівень розвитку і використання ІКТ в світі дуже нерівномірно, зокрема, інформаційні проблеми 60% населення перебувають на зовсім іншому рівні. Проте, це не означає, що вони не існують. Людина завжди "приречена" на пошук, оцінку та захист інформації (різниця полягає тільки за своїм змістом – інформація про місця для полювання, джерело води, інше плем’я чи щодо комерційної таємниці і персональних даних), тобто, інформаційну діяльність, яка нерозривно пов’язана

з інформаційною безпекою. Тільки от за умови формування інформаційного суспільства значення останньої невпинно зростає. Переважна більшість наукових праць на тему інформаційної безпеки починається з обґрунтування її актуальності, посилення проникнення інформаційних технологій в усі сфери життя суспільства, а також становлення інформаційного суспільства як нового етапу розвитку (типу) суспільства, в якому питання інформаційної безпеки набуває нової значимості і становить предмет правового регулювання, один з основних напрямів гарантування національної безпеки та безпеки держав, а також передумовою дотримання прав і свобод людини і громадянина. Таким чином, феномен інформаційної безпеки розглядається через призму практично-діяльнісного відношення людини до держави і суспільства, опираючись на потребах і інтересах об'єктів і суб'єктів безпеки. Безперечно, усвідомлена безпека здатна чинити вирішальний вплив на зміст і розвиток суспільних процесів. Цим обумовлена актуальність дослідження інформаційної безпеки як наукової категорії і як суспільного явища.

Інформаційне протистояння, як і кожне інше, є природно обумовленим елементом конкуренції сучасного глобалізованого світу, тому проблематика інформаційної та кібернетичної безпеки набуває особливої ваги з метою встановлення балансу інтересів особи, суспільства, держави та міжнародного співтовариства. Інформаційна безпека як наукова категорія є тлумачена на різні способи. Мають місце як доктринальні, енциклопедичні, так і нормативно-правові визначення. При цьому, методологічні підходи, логічні способи їх утворення і закріплення, сфери існування і прикладного використання суттєво відрізняються. Це пов'язано також із тим, що сама категорія безпеки неоднозначна і визначається в залежності від наукової області, в якій він вивчається. Характерною особливістю наукового пізнання є прагнення такого знання, яке ми могли б кваліфікувати як істинне. Історія філософії і науки дає нам привід сумніватися у можливості одностайного тлумачення такого феномена, як істина. Враховуючи, що основною проблемою філософії є відношення "людина – світ, процес усвідомлення людиною сутності світу свого

буття і своєї власної сутності в їхньому взаємозв'язку", необхідним вбачається усвідомлення внутрішнього змісту, ознак і особливостей, поняття, що досліджується [48]. Зокрема, в філософському розумінні необхідно звернутись до трьох основних аспектів відображення предмету в теорії - онтологічного, гносеологічного і логічного. Онтологічний аспект полягає в тому, що зміст філософії є об'єктивним за своїм походженням і відображає об'єктивно існуюче відношення "людина – світ".

Філософія ж, як специфічна форма усвідомлення людиною свого буття, як форма суспільної свідомості, претендує на те, щоб дати людині знання про світ і про саму людину в їхньому бутті [42]. Безпека з точки зору філософії є формою і способом існування. Структура явища повстає в динаміці історичного процесу. Її сутність поєднує внутрішній зміст і зовнішні прояви, відображаються в істотних властивостях, які визначають тенденції його розвитку. Таким чином, єдина сутність може знайти відображення і бути пізнаною через множину явищ. Гносеологічний аспект відображення предмета в теорії полягає в тому, що світ відображається у свідомості людини не дзеркально, не як результат споглядального сприйняття дійсності, а через призму практично-діяльного відношення людини до світу і до самої себе, через призму потреб і інтересів. Саме пізнавальне відношення людини до дійсності є практичним за своєю природою. В основі відношення людини до світу лежать її потреби й інтереси. Вони можуть бути задоволені тільки в процесі практичного освоєння людиною дійсності [82]. У загальному соціологічному розумінні категорія «безпека» характеризує певний стан людського суспільства, при якому забезпечується його нормальне існування і стабільний розвиток. У соціальних моделях під безпекою розуміють розв’язання проблеми умов оптимального функціонування суспільства та його прогресивного розвитку. У широкому філософському та світоглядному аспекті безпека являє собою важливе питання як для наукового пізнання, так і практики існування соціуму в масштабах окремої держави та планети загалом [36]. Безпека є усвідомленим явищем для конкретного суб’єкта суспільних відносин. Вона виступає як прояв

активної взаємодії і відносної самостійності суспільної свідомості у відношенні до суспільного буття. Оскільки безпека є усвідомленим явищем, можна зробити висновок, про усвідомлення факторів, що негативно на неї впливають, і необхідності її забезпечення з метою збереження максимальної життєздатності соціальної системи, з урахуванням реальних та потенційних загроз або ризиків її існуванню та розвитку. У основі будь-якої безпеки як системи мають місце життєво важливі інтереси особи, нації, держави чи міжнародного співтовариства. В цьому, як процесі, проявляється розуміння, 19 сенс, необхідність усвідомленого оволодіння ідеєю безпечного існування заради подальшого існування чи розвитку соціальної системи. Розкриваючи філософські проблеми безпеки як соціального явища, слід відзначити, що поняття про безпеку і усвідомлення її необхідності проявляється як на чуттєвому (підсвідомому), так і на раціональному рівнях. В дослідженнях К. Лідерман, польський безпекознавець, стверджує, що в той час як забезпечення стосується в більшій мірі заходів (технічних, організаційних, правових тощо), то безпека – суб'єктивного відчуття [66].

Передчуття, негативні емоції, відчуття небезпеки, почуття необхідності самозахисту з подальшим усвідомленим формуванням системи охорони та захисту є проявом багатства різноманітності людської природи, невичерпності людських якостей. Тобто, безпека знаходить відображення у свідомості суб'єкта суспільних відносин як динамічний процес, що має низку варіативних детермінант - стан, рівень розвитку системи, в тому числі культурності й цивілізованості. Тому обґрунтованою є постановка проблеми виявлення і розкриття сутнісних ознак безпеки як соціального феномену. До них можуть бути віднесені усвідомлена самодостатність, здатність до самозбереження, захищеність від загроз, гарантованість власного існування і т. і. В практичній діяльності (в політичній, економічній, правовій, культурній сферах) мають місце статичні ознаки: визначення стану захищеності від загроз у просторі, часі та за колом осіб. У практичній площині існування соціальних систем безпека не є абстрактним явищем, відірваним від конкретних умов життя. Її зміст

узалежнений від конкретних соціальних умов. Безпека виступає як потреба існування особи, нації, держави з огляду на те, що її функціонування пов'язане з задоволенням найважливішої потреби людини. Безпека співвідноситься із самою можливістю життя, виступає умовою його збереження і основний критерій ймовірного розвитку. В сучасній науковій літературі має місце дискусія про те, що постановка самої проблеми безпеки обумовлена усвідомленням загроз, тобто проблема безпеки, безпечного існування соціальної системи пов'язується до антиподу - небезпеки чи загрози. Такий методологічний підхід обґрунтовує, якщо відсутня 20 небезпека, то зникає потреба в безпеці, а, отже, і в забезпеченні існування системи охорони, оборони, протидії і захисту. Лише наявність небезпеки обумовлює таку потребу. Подібну позицію висловлює К. Лідел, польський юрист, фахівець з міжнародного тероризму. На його думку, безпека і загрози є нерозривно пов'язаними явищами. Вони становлять протилежні одиниці виміру соціальних явищ [61].

Сутність іншого підходу можна виразити через відомий вислів: прагнеш до миру – готуйся до війни. Тобто, що безпека повинна мати місце завжди, навіть за відсутності очевидних небезпек або загроз. З філософської точки зору, суть проблеми полягає в тому, що оскільки безпека є усвідомленим явищем, то вона повинна бути і збереженою від усіляких можливих негативних втручань, негараздів, впливів тощо. Це чітко окреслює активний зміст суспільної свідомості, що здатна прогнозувати, передбачити і уявити небезпеки. З цього слідує, що самозбереження є здатністю і основною властивістю свідомості. Прагнення до безпеки є виразом розумності соціальної системи, проявом усвідомленого змісту її буття, її суспільного і морального сенсу. Безпека при такому підході виступає як невід'ємний атрибут існування. Автор власне підтримує цю позицію, що не слід пов'язувати існування безпеки як явища виключно зі своїм антиподом – небезпекою. Усвідомлення проблеми безпеки набуває повноти з огляду на діалектику життя. Повноцінний розвиток не є можливим без безпеки. Отже, безпека виступає і як гарантія сталого розвитку

будь-якої суспільної системи: набуття нею нових ознак, якостей тощо. Популярна концепція сталого розвитку хоча в первинному своєму розумінні насамперед стосувалась необхідності встановлення балансу між задоволенням сучасних потреб людства і захистом інтересів майбутніх поколінь, акцентуючись на потребі в безпечному і здоровому довкіллі [43].

Водночас, на сьогодні, основою такого розвитку визнається системний підхід та сучасні інформаційні технології, за допомогою яких є можливим моделювання різних варіантів напрямків розвитку, прогнозування їх результатів та вибір оптимальних, в тому числі з огляду на безпеку. 21 Безпека є поняттям, що окреслює стан стабільності, спокою і відсутності загрози. Вона має суб'єктивний характер, виступає однією з підставових потреб людини, суспільних груп і держав. Охоплює задоволення таких потреб як існування, виживання, цілісність, ідентичність, незалежність, спокій (мир), наявність і стабільність розвитку [67]. Пронизуючи всі напрями діяльності соціальної системи і визначаючи її ефективність, функція безпеки в пізнавальному філософському аспекті виступає в якості методологічної основи для формування теоретичних підходів і практичних дій особи, суспільства, держави. Поняття безпеки при такому підході виступає інструментом пізнання сутності існування системи як цілісного організму, методологічною базою аналізу якості життєдіяльності конкретної суспільної системи, її ефективності та стійкості до різних загроз, спрямованих на порушення бажаного її стану. Г.А. Пастернак-Таранушенко вважає, що безпека – це стан об'єкта захисту, що відрізняється динамічною стабільністю та своєчасною можливістю вплинути на хід подій з метою збереження цього об'єкта [302]. По суті ним зроблена спроба через теорію статики довести теорію динаміки безпеки. Але за будь-яких умов у сучасних умовах задоволення потреби у безпеці на всіх її рівнях (індивідуальному, суспільному, національному, міжнародному) передбачається застосування системного підходу щодо всебічного врахування значної множини факторів, одним з яких є важливість вибору такої стратегії розвитку соціальної системи, за якої досягається гармонія її взаємовідносин з іншими

соціальними системами на основі ідей співіснування, взаємодії, співпраці. Про це більше розглянемо в підрозділі «Інформаційна безпека як системне явище». Таким чином, безпека, в одному аспекті – це тенденції розвитку й умови життєдіяльності соціуму, його структур, інститутів, що визначаються відповідними настановами (політичними, правовими та іншими), за яких забезпечується збереження їх якісної визначеності та вільне, яке відповідає їх природі, функціонування. В другому – це захищеність вказаного функціонування від потенційних і реальних загроз [43]. Третій, логічний аспект розкривається через результат практичнодіяльнісного і пізнавального відношення до дійсності, відображеного в змісті філософського знання, яке виражається за допомогою понятійно-категоріального апарату. Поняття і категорії дозволяють окреслити ступінь усвідомлення людиною власного ставлення до світу і до себе. Зміст та структура понятійнокатегоріального апарату відбивають динаміку розвитку самої дійсності, людини, і їх взаємозв'язку [82].

Етимологічно термін "безпека" ("security") походить від латинського виразу "sine cura", що означає без (sine) і догляду, турботи, занепокоєння, заклопотаності (cura). Подібною є етимологія українського терміну «безпека». Академік Тихий В.П. пропонує наступний етимологічний аналіз слова «безпека» [49].

Слово «безпека» створено з прийменника «bez» і основи іменника «peka», пов’язаного з дієсловом «pekti» (українською – «пекти»)[135]. Прийменник «без» має загальнослов’янський індоєвропейський характер. Його вихідне, початкове значення за одними джерелами – «поза», за іншими – «крім»[161]. Слово «пека» походить від слова «пек», яке запозичене з голландської мови («pek» – смола). У старослов’янській мові – «пькъ», «пькълъ» – смола; пекло. У християнстві грішники киплять у пеклі в смолі, горять у вічному вогні; через те в народній етимології слово «пекло» пов’язується з дієсловом «пекти». Пекло – найнебезпечніше місце [135].

Етимологія безпеки пов’язана з міфом про Пека – слов’янського бога пекла. У давньоукраїнській міфології Пек – бог пекла, а також війни, кривавих бійок, кровопролить та всілякої біди, син Чорнобога і Марі. Згідно з повір’ям він був кровожерний, страхітливий, підступний, нещадний, але лякливий, надто боявся Чура (звідси давнє прислів’я «Чур тобі, Пек»). «Пекло» – царство Пека, страхітливе підземелля, куди «провалювалися» душі грішників після своєї смерті. За давніми міфами пекло мало дванадцять ярусів (дванадцять проваль одне нижче одного, з кривими горловинами між ними; чим більше гріхів мала людина, тим важчої була її душа і тим глибше вона падала). Наші пращури вірили, що Пек затягував до пекла і праведників, добрих людей. З усіх богів Вирію лише Чур міг проникати в пекло й відбивати в Пека невинні душі добрих людей чи своїх 23 лицарів-побратимів, повертати їх на землю чи до Вирію. Битва Чура з Пеком у підземеллі за уявленням давніх українців призводила до землетрусів. Спровадити до пекла (на шибеницю і т. ін.) означає заподіяти кому-небудь смерть [312,]. В староросійській мові загальнослов’янське «pekti» існувало в двох похідних формах: «пекъ» (пека) – «жара, спека», і «печа» - турбота, опіка (рос. попечение) [22].

Від цієї другої форми пішло дієслово «обеспечивать», тобто усувати турботи, створювати умови, коли «не пече». Цікаво, що в сучасній польській мові досі залишилась форма «печа» (piecza) – догляд, опіка, турбота». Власне його однокореневим є польське «bezpieczeństwo» - «безпека». Таким чином, етимологічне походження поняття «безпека» узалежнює його від небезпек, загроз і ризиків. Але в сучасній науковій думці такий підхід є лише одним з існуючих.

Розвиток і удосконалення знання не може успішно здійснюватися без удосконалення, розвитку понятійного апарату, у якому фіксуються результати освоєння світу, ступінь проникнення людського пізнання в сутність предметів, процесів об'єктивної дійсності. Зневажливе ставлення до розробки понятійного апарату, недбалість у використанні термінології часто призводять до значних втрат у дослідженні явищ дійсності і навіть до помилок, до нерозуміння

дослідниками один одного [22]. Тому так важливим, на нашу думку, є інтегрований підхід до вивчення феномену інформаційної безпеки, що ґрунтується на суспільно-історичній і соціально-діяльнісній сутності людини, в діалектичній єдності людини і світу. Внаслідок практичної зумовленості пізнавального ставлення людини до світу теоретичне відображення дійсності у свідомості наповняється конкретним змістом. Тому і зміст філософського знання містить у собі відображення світу не у всій його загальності і багатогранності, а в тій мірі, у якій дійсність включається в сферу практично перетворювальної діяльності людини. На цій основі складається і специфічне бачення світу в рамках буття людини [482].

Якщо в такому випадку світ виступає як світ буття людини, то безпека у сучасних соціальних системах виступає основним поняттям оточуючого 24 середовища, яка характеризує певний стан буття, при якому забезпечується його нормальне існування та стабільний розвиток [36]. Історія виникнення та розвитку поняття «безпека» охоплює значний проміжок часу, що фактично збігається з виникненням та розвитком людства [3].

Трансформація категорії безпеки відбулась разом із визначенням довкілля, пізнанням природних процесів, поширенням науково-технічних знань, культури тощо. В основі фундаментального розуміння цієї категорії лежить утопічна ідея, яка протягом століть мотивує науковців, - це ідея можливості контролювати майбутнє, прогнозувати майбутні події та прораховувати ймовірні сценарії розвитку з максимальною вірогідністю, основною метою якої є створення ідеальних умов розвитку людства [36]. У розуміння ідеального входить поняття безпечного, що визначає їх взаємодоповнюваність у системі соціальних відносин [3].

Згідно енциклопедичному визначенню під категорією «інформаційна безпека» може розумітись: законодавче формування державної інформаційної політики; створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;

гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; всебічний розвиток інформаційної структури; підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України; створення і впровадження безпечних інформаційних технологій; захист права власності всіх учасників інформаційної діяльності в національному просторі України; збереження права власності держави на стратегічні об'єкти інформаційної інфраструктури України; охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою; створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом; захист національного інформаційного простору України від розповсюдження 25 спотвореної або забороненої для поширення законодавством України інформаційної продукції; встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів із іноземними державами; законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [216]. Вчена, фахівець з інформаційного права Бачило І.Л. акцентує увагу на багатоплановості поняття «інформаційна безпека» і відносить до кола питань, що ним охоплюються: захист відкритої інформації, охорону державної таємниці, забезпечення захисту інформації з обмеженим доступом, окрім державної таємниці, страхування інформації і інформаційних ресурсів [34].

На початках становлення наукового розуміння категорії спостерігалось ототожнення «інформаційна безпека» і «безпека інформації». Тер-Акопов А.А. під інформаційною безпекою розуміє також стан захищеності інформації, що забезпечує життєво важливі інтереси людини [45]. При цьому таке ототожнення мало місце як в працях вітчизняних науковців, так і зарубіжних. Яскравим

прикладом може служити визначення, що містилося в одному з перших перекладених на російську мову видань в СРСР щодо методів захисту інформації Л.Дж. Хоффмана: «інформаційна безпека – стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [495]. В дослідженнях науковців досі можна зустріти подібне безпідставне ототожнення. Редакція наукового журналу «Безпека інформації», який було засновано у 1995 р., визначила основною метою журналу висвітлення результатів наукових досліджень та поширення інформації з усіх аспектів інформаційної безпеки [39].

Водночас, переважна більшість дослідників чітко розмежовує ці категорії, опираючись на тому, що при визначенні безпеки інформації об'єктом виступає власне інформація, а у випадку інформаційної безпеки – безпека як частина цілого [81]. Небезпідставною вбачається позиція Фурашева В.М., що при вирішенні проблем інформаційної безпеки важливе місце становить дилема між 26 гарантованістю прав і свобод суспільства збирати, зберігати, використовувати і поширювати інформацію та об'єктивного вимушеного правового обмеження, неможливе без чіткого визначення об'єктів та суб'єктів права у всій його сукупності, виходячи із сутності явища, процесу, процедур тощо [46].

Близькою за змістом видається позиція Дзьобаня О.П. і Пилипчука В.Г., які визначають інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства та держави в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, що забезпечує їх сталий розвиток [116]. Певною мірою розвиває такий підхід, коли під інформаційною безпекою пропонує розуміти результат управління реальними та (або) потенційними викликами і загрозами щодо захищеності важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, у т.ч. з використанням правових методів [117]. Богуш В. визначає, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій,

держави [55]. Дуже близьким семантично є визначення Фісуна Ю.А. - „стан захищеності інформаційного середовища, що відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз” [41]. В межах даного напряму існує визначення інформаційної безпеки як стану, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів та установ, за яких здійснюється збереження якісної, з об’єктивно обумовленими інноваціями в ній, вільне, відповідне власній природі функціонування інформації. Окремі представники цього напряму розглядають інформаційну безпеку через відсутність небезпеки, тобто чинників та умов, що загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища.

Прибічники такого підходу вважають інформаційну безпеку лише станом чи процесом захищеності особи, суспільства, держави від реальних або потенційних загроз [148]. Наступний погляд передбачає, що у самому загальному вигляді під інформаційною безпекою можна розуміти здатність суб'єкта зберігати свої системостворюючі властивості, основні характеристики при патогенних дезорганізуючих, деструктивних впливах на кіберпростір, інформаційнокомунікаційні технології. На думку прибічників цього погляду, серед яких Ліпкан В.А. [236], безпека і забезпечення безпеки становлять собою різні поняття, через те, що безпека виражає характеристику стану соціальної спільноти, тоді як забезпечення безпеки — діяльнісну характеристику, тобто діяльність органів державної влади і управління з підтримання безпеки. Таким чином, безпека виступає основою цілепокладання політики, а забезпечення безпеки — як діяльність з досягнення безпечного стану суспільства або соціальної групи. Горбатюк О.М. вважає, що інформаційна безпека – представляє собою стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [96]. Ярочкін В.І. визначає безпеку як стан захищеності особи, суспільства та

держави від зовнішніх та внутрішніх небезпек та загроз, що базується на діяльності людей, суспільства, держави, світового співтовариства щодо виявлення (вивчення), попередження, послаблення, ліквідації та відбиття небезпек і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятну шкоду, закрити шлях для прогресивного розвитку [52]. Гурковський В.І. визначає національну інформаційну безпеку України як суспільні відносини, пов’язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в 28 інформаційному просторі, що є необхідною умовою збереження та примноження духовних та матеріальних цінностей нації, прогресивного розвитку України, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [103]. Литвиненко О. пропонує під інформаційною безпекою слід розуміти одну із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [232]. Кормич Б. А. визначає інформаційну безпеку як захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави. Він також виділяє ряд основних ознак інформаційної безпеки, що обумовлюються специфікою її об'єкта: зони інформаційної безпеки перебувають на перехресті функції національної безпеки та інформаційної функції держави; питання інформаційної безпеки держави носить екстериторіальний характер; суспільні відносини, що входять до сфери інформаційної безпеки, є неоднорідними і різноплановими; компетенція держави у сфері інформаційної безпеки обумовлюється конкуренцією між інформаційними правами особи та функціями держави і її органів по регулюванню інформаційних процесів; у демократичному суспільстві державне регулювання інформаційної сфери

можливе лише шляхом встановлення правових норм; політика інформаційної безпеки носить багатовекторний характер, її головними складовими (векторами) є: (1) регулювання інформаційних відносин з метою забезпечення національної безпеки, територіальної цілісності та громадського порядку, підтримання законності; (2) регулювання інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я та моральності; (3) регулювання інформаційних відносин у сфері комерційної інформації [208, с.93].

Нижник Н.Р. під інформаційною безпекою розуміє стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [276]. 29 Петрик В. М. зазначає, що природні явища "безпека" і "небезпека" існують в діалектичній взаємозалежності, тобто у природі не існує окремо "стану безпеки" та "стану небезпеки" [306]. Також заслуговує на увагу точка зору О. Логінова, який стверджує, що не слід обмежуватись поняттям «стан» при визначенні категорії «інформаційна безпека», а стверджує, що вона є процесом. Зокрема, на його думку, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності органів виконавчої влади [239].

Тихомиров О.О., опираючись детально розроблений в теорії держави і права діяльнісний підхід виокремлює положення, що визначають своєрідність його застосування для дослідження державно-правового забезпечення інформаційної безпеки: суб'єктивний аспект забезпечення інформаційної безпеки як діяльності визначається тим, що воно здійснюється певними суб'єктами (державними і недержавними), метою і результатом дій яких є стан інформаційної безпеки, а ефективність цих дій залежить від усвідомлення суб'єктами соціальної зумовленості, спрямованості дій на задоволення відповідних суспільних і індивідуальних інформаційних потреб, необхідності їх реалізації у взаємодії з іншими соціальними суб'єктами тощо; об'єктивність

забезпечення інформаційної безпеки визначається конкретними економічними, історичними, соціальними, культурними умовами її здійснення, а отже залежить від реального стану функціонування держави та інститутів громадянського суспільства, рівня розвиненості інформаційного суспільства, інформаційних процесів і технологій, інформаційної культури населення тощо; регулятивна площина забезпечення інформаційної безпеки орієнтує на осмислення впорядкування забезпечення інформаційної безпеки різноманітними соціальними правилами, домінуючим серед яких є право, а також власне нормами інформаційного спілкування та внутрішніми переконаннями суб'єктів забезпечення інформаційної безпеки; процесуальний ракурс вивчення діяльності щодо забезпечення інформаційної безпеки передбачає осмислення послідовності використання різноманітних 30 засобів, способів, а в результаті - виокремлення відповідних стадій, що складають процес здійснення діяльності або її окремих фрагментів[461]. Російські дослідники А. Урсул і О. Романович переконані, що забезпечення безпеки не зводиться тільки до захисту; ідея національної безпеки тісно пов’язана з концепцією стійкого демократичного розвитку, є її невід’ємною частиною і водночас умовою її реалізації. Такий підхід значно розширює поняття «інформаційна безпека» за рахунок включення в нього «здатності держави ефективно захищати національні інтереси і цінності» [47]. Наливайко Л. Р. вважає, що інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [267].

Під час розробки проекту Закону України «Про засади інформаційної безпеки України» було запропоноване наступне визначення: інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг

інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [350]. Проте, ця пропозиція досі знаходиться на розгляді. Різноманітність підходів до визначення категорії «інформаційної безпеки» вказує, що воно являє собою одну з важливих та багатогранних концепцій в науці та інших сферах людської діяльності. Зміст і складність цієї концепції є також притаманною складовою сучасного інформаційного суспільства. Аналіз різних підходів до визначення категорії інформаційної безпеки дозволяє зробити висновок про недоцільність суворого дотримання однієї позиції.

Найбільш відповідним, на нашу думку, є комплексний підхід, згідно з яким інформаційна безпека визначається через її істотні риси, найбільш важливі основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем. Таким чином, онтологічне розуміння інформаційної безпеки опирається на ціннісному вимірі об’єкта безпеки. Тобто, коли йдеться про інформаційну безпеку людини – то це насамперед потреби людини, можливість реалізації яких в правовому полі закріплюється через її права і свободи. В той час гносеологічно зміст інформаційної безпеки зводиться, з однієї сторони, до небезпек і загроз, що виникають і впливають на існування об’єкта, а з іншої – до діяльнісної складової – можливостей суб’єктів щодо створення безпечних умов існування об’єкта інформаційної безпеки. Логічний зміст інформаційної безпеки має особливе значення в правовій площині. Адже нормативне закріплення як правової категорії означає, що на ньому буде будуватись система інформаційної безпеки. Через закріплення у відповідних правових нормах виконуються регулятивну і охоронну функції права, а саме закладаються основи захисту об’єктів інформаційної безпеки і правового регулювання діяльності суб’єктів інформаційної безпеки. Легітимізуючи категорію «інформаційна безпека» в законодавстві як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність

інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації», в один ряд поставлені життєво важливі інтереси людини, суспільства і держави, які в реальності часто є суперечливими і неспіврозмірними. Визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління.

1.2. Ґенеза суспільних відносин щодо інформаційної безпеки

Усвідомлення людиною цінності певного виду інформації, особливостей наявних процесів комунікації, а також можливостей завдання шкоди особистим і суспільним інтересам шляхом інформаційних впливів або використання інформаційного обміну обумовили усвідомлення інформаційної безпеки. Проте, 32 на нашу думку, не слід говорити про її появу – адже безпека, як умова існування і розвитку людини, завжди була однією з базових її потреб. Водночас, безпека є невід'ємною властивістю соціальних систем (в т.ч. суспільства), яким може бути завдано шкоди шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між всіма елементами. Інформаційна безпека людини, водночас, є і станом, і процесом, оскільки виступає невід'ємною частиною життя, в якому людина постійно перебуває під дією конкретних інформаційних впливів. З огляду на вищезазначене, в цій праці взято до уваги історичні передумови захисту інформації, використання інформаційних впливів на людину в інтересах держави та інших суб'єктів, а також зародження інформаційних прав людини, зокрема, права на захист персональних даних та доступ до публічної інформації. Очевидно, цим переліком не вичерпується проблема, проте обмежений обсяг роботи і цілі нашого дослідження обумовили

саме такий вибір. Історія захисту інформації. Початок історії захисту інформації вчені пов’язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю. Практично одночасно з народженням писемності виникли перші методи захисту інформації, як шифрування і приховування. Один з найстаріших шифрованих текстів з Месопотамії (2000 рр. до н. Е..) Являє собою глиняну табличку, що містить рецепт виготовлення глазурі в гончарному виробництві, в якому ігнорувалися деякі голосні і приголосні і вживалися числа замість імен.

З розвитком суспільства удосконалювалися і способи добування необхідної інформації. До IV століття до н. е. Схід значно випередив Захід в мистецтві розвідки. Сунь Цзи писав: «Те, що називають передбаченням, не може бути отримано ні від духів, ні від богів ... ні за допомогою розрахунків. Воно повинно бути видобуто від людей, знайомих з положенням противника»[44]. Бажанню здобувати конфіденційну інформацію завжди протиставлялось не менше бажання протилежного боку захистити цю інформацію. Стародавні способи захисту інформації по суті перетривали до сучасності, удосконалюється 33 лише техніка їх реалізації. Наприклад, з метою приховування самого факту наявності інформації у Стародавньому Римі повідомлення, написане на дошці, приховували від сторонніх очей, заливши його воском. У Стародавній Греції обривали раба, писали на його голові і, коли волосся відростало, відправляли до адресата. У середні віки винайдено тайнопис і повідомлення приховували за допомогою невидимих хімічних засобів. В сучасних умовах поширені такі стеганографічні методи, як приховування змісту повідомлень в малюнках, телевізійних і аудіосигналах тощо [417]. Паралельно розвивалися методи шифрування і кодування (криптографічні методи), історія яких починається з часів виникнення писемності в Стародавньому Єгипті та Китаї. Окремі автори процес розвитку захисту інформації розподіляють на відносно самостійні періоди, в основу яких покладено або еволюцію видів носіїв інформації, або розвиток засобів

інформаційних комунікацій. Так, Сьомкін С.Н. виділяє три періоди розвитку засобів і методів захисту інформації [75]. Перший період визначається початком створення осмислених і самостійних засобів і методів захисту інформації і пов'язаний з появою можливості фіксації інформаційних повідомлень на твердих носіях. Тобто з винаходом писемності. Одночасно з можливістю збереження і переміщення даних виникла проблема, як зберегти в таємниці конфіденційну інформацію, яка існує вже окремо від джерела. Тому практично одночасно з народженням писемності виникли такі методи захисту інформації, як шифрування і приховування. Один з найстаріших шифрованих текстів знайдений в Месопотамії (XX ст. до н. Е.). Він являє собою глиняну табличку і містить рецепт виготовлення глазурі в гончарному виробництві, в якому ігнорувалися деякі голосні і приголосні, а замість імен вживалися числа. Другий період (приблизно з середини XIX ст.) обумовлений появою технічних засобів обробки інформації і можливістю збереження і передачі повідомлень за допомогою таких носіїв, як електричні сигнали і електромагнітні поля (наприклад, телефон, телеграф, радіо), а отже проблемами захисту від так званих технічних каналів витоку (побічних випромінювань, наведень і ін.). З'явилися способи шифрування повідомлень в реальному масштабі часу (в 34 процесі передачі по телефонним і телеграфним каналах зв'язку) і т. Д. Крім того, це період активного розвитку технічних засобів розвідки, що багаторазово збільшили можливості промислового і державного шпигунства. Третій період Сьомкін пов’язує з масовою інформатизацією суспільства, тому, на його думку, історія найбільш інтенсивного розвитку захисту інформації пов'язана з впровадженням автоматизованих систем обробки інформації і вимірюється періодом понад 50 років.

Враховуючи вплив на трансформацію ідей інформаційної безпеки, в розвитку засобів інформаційних комунікацій автори іншого російського дослідження виділяють сім етапів [175]:

I етап (до 1816 р.) використання природних засобів інформаційних комунікацій. В цей період основне завдання інформаційної безпеки полягало в

захисті відомостей про події, факти, майно, місцезнаходження тощо, що мали для людини особисто або мікросоціуму, до якого вона належала, життєве значення.

II етап (починаючи з 1816 р.) пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку.

Для забезпечення безперешкодності радіозв'язку необхідно було використовувати кодування повідомлення (сигналу) з подальшим його декодуванням.

III етап (починаючи з 1935 р.) пов'язаний з появою засобів радіолокацій і гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокацій від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.

IV етап (починаючи з 1946 р.) пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами обмеження фізичного доступу до устаткування засобів обробки і передачі інформації.

V етап (починаючи з 1965 р.) обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки вирішувалися, в основному, методами і способами фізичного захисту засобів 35 обробки і передачі інформації шляхом адміністрування і управління доступом до мережевих ресурсів.

VI етап (починаючи з 1973 р.) пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці серйознішими суттєво ускладнились і потрібно було розробити нові критерії безпеки. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки — найважливішою і обов'язковою

складовою національної безпеки. Формується інформаційне право — нова галузь міжнародної правової системи.

VII етап (починаючи з 1985 р.) пов'язаний із створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення.

Автори цього дослідження припускають, що черговий етап розвитку інформаційної безпеки, буде пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення міжнародної макросистеми інформаційної безпеки людства. Історія інформаційної безпеки на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загальновизнаним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на небезпеку, а заздалегідь поширені чутки, перебільшення і дезінформація призводили до паніки [293, с. 11].

Зазначимо, що в 988 р. Володимир розпочав релігійну реформу, і тому ще один вид інформації про віросповідання теж підлягав спочатку охороні. Перші князі тримали своє віросповідання в секреті, зокрема Ольга, а сам Володимир не відразу наважився 36 прийняти християнське віровчення попри неодноразові пропозиції Візантії. За Володимира та Ярослава особливого розмаху набуває зовнішньополітична, дипломатична діяльність держави, саме інформація про дипломатичні відносини підлягала охороні. Деякі науковці висловлюють припущення, що вже в період Київської Русі з'явилися державні службовці, які здійснювали захист окремих видів інформації. Можливо це були

представники молодшої дружини, а саме: отроки, боярські діти та пасинки. Основним засобом зв'язку в той час були спеціальні князівські гінці, «люди піші та кінні», і «вірні голови» (люди з князівської дружини) [20, с.10]. Використовувалися й інші способи зв'язку: оптична сигналізація за допомогою багать і димів, сигнальних труб і свистків [21, с. 417]. Для забезпечення конфіденційності інформації, що передається використовувалися різні методи. Найбільш важливі повідомлення заучувалися гінцем напам'ять. При цьому часто використовувалися натяки, умовні слова. Суть методу полягала в тому, що зміст переданого повідомлення могла зрозуміти тільки посвячена людина.

Надалі, в криптографії такий спосіб забезпечення секретності отримав назву «жаргонного коду» і застосовується досі. Так, наприклад, на жаргоні багатьох розвідок слово «хворіти» означає «арешт» або «взяття під варту»; лікарня - в'язниця; «лікар» - контррозвідка [21, с. 423] Таким чином, повідомлення «Майкл арештований контррозвідкою. Йому загрожує ув'язнення набуває досить «невинного вигляду»: «Майкл захворів. Вчора був лікар і порадив йому лікуватися в лікарні» [93]. Використовувано і так звану «пташину мову» коли в усне повідомлення вставлялися частки-паразити. Подібні способи захисту інформації з давніх часів були поширені не тільки у державних службах, а й серед представників кримінального світу в різних країнах. Для захисту письмових повідомлень використовувалася фізичний захист, стеганографія і шифрування. В якості гінців використовувалися фізично міцні люди, вони були добре озброєні, нерідко гонець слідував в супроводі охорони. Стеганографічний метод широко використовувався - повідомлення приховувались в одяг, в підошви і каблуки взуття [21]. На жаль, шифровані документи, що містять інформацію державного характеру, що відносяться до епохи Київської Русі поки не виявлені. Однак зберігся ряд пам'ятників давньоруської писемності, в яких є зашифровані фрагменти. В основному це літописи і тексти релігійного змісту. У цих джерелах тайнопис застосовується не стільки для забезпечення секретності, скільки для того, щоб підкреслити важливість того чи іншого фрагмента, а також увіковічити ім'я автора або

переписувача. Саме ці документи дають можливість описати давньоруські системи шифрування. В Литовсько-польській державі, до складу якої увійшли українські землі, найважливішою так само визначалась військова інформація, інформація про особу князя (потім короля), і в Литовському статуті Великого князівства литовського (1588 р.) з'являється новий вид інформації, що охоронялася, - державна таємниця.

В Речі Посполитій пошуком і знешкодженням шпигунів з метою захисту інформації займалися призначені королем відповідальні особи з його найближчого оточення. В Російській імперії було встановлено кримінальну відповідальність за розголошення такого виду інформації як державна таємниця. Зокрема, у «Соборному Уложении» (1649 р.) була стаття, що визначала смертну кару за такі дії [29].

Водночас, централізованої системи охорони державної таємниці не існувало. Найбільш розвиненою була система захисту військової інформації. Її основними напрямами були створення і вдосконалення системи контррозвідувальних органів; організація комплексної системи захисту інформації, що містить військову таємницю; вдосконалення системи фельд'єгерського зв'язку; організація військової цензури. Наступний період (з середини XIX ст.) пов'язують з появою технічних засобів обробки інформації та передачі повідомлень за допомогою електричних сигналів і електромагнітних полів (наприклад, телефон, телеграф, радіо). У зв'язку 38 з цим виникли проблеми захисту від технічних каналів витоку. На початку XIX століття криптографія збагатилася чудовим винаходом - система шифрування "дисковим шифром", автором якого вважається екс-президент США Томас Джефферсон. Суттєво вдосконалено систему охорони інформації та її нормативно-правове забезпечення було у XX сторіччі, чому суттєво посприяли дві світові війни. За час існування проблеми захисту інформації змінилися як уявлення про її сутність, так і методологічні підходи до її вирішення. Правове забезпечення захисту інформації у XX сторіччі стало складовою частиною ширшої категорії - інформаційної безпеки. Під юридичними аспектами

правового забезпечення захисту інформації почали розуміти сукупність нормативно-правових актів, за допомогою яких узаконювались:

1) правила захисту конфіденційної інформації;

2) заходи відповідальності за порушення правил захисту інформації;

3) вирішення питань організаційно-правового забезпечення захисту інформації;

4) процесуальні процедури вирішення ситуацій [38].

Хоча правова регламентація охорони інформації недержавного і невійськового змісту має місце лише з другої половини XX сторіччя, проте зародження окремих її видів сягає стародавніх часів. Так, Ф. Вальтер зазначає, лікарська таємниця має глибоке коріння, ведучи свій початок від часів стародавнього жрецтва (Єгипет, Індія), коли лікування являло собою релігійний акт і жерці, які займалися лікуванням, огортали мистецтво лікування таємницею [110]. В Стародавній Індії існувало поняття лікарської таємниці: відомості, отримані від хворого, не розголошувалися, якщо вони могли справити погане враження на близьких людей. Лікар не повинен був повідомляти пацієнту про свої спостереження, які могли негативно вплинути на душевний стан хворого й перешкодити одужанню. Це відповідало аюрведним уявленням про необхідність душевного спокою для збереження здоров'я [56]. Наступним витком у спіралі розвитку лікарської таємниці стала клятва Гіппократа, у якій ідеться про таке: «Про що б під час лікування і також без лікування я не побачив або не почув щодо життя людей із того, що не потрібно розголошувати, я промовчу про те, вважаючи подібні речі таємницею» [85]. Усередньовіччі поняття «лікарська таємниця» відображено в статутах Паризького медичного факультету 1600 р., які забороняли видавати таємниці хворих. Крім того, у середньовічній Європі особливою пошаною користувалися «Канони медицини» арабського мислителя Авіценни, у яких, зокрема, йдеться про збереження лікарем у таємниці того, що йому відомо про хворого [7].

Проте, у клятві європейських лікарів, яка відома з VI ст. н. е., відсутні згадки про таємницю. Так тривало до XVI ст., коли в різних країнах Європи

(Італії, Швейцарії, Німеччині, Франції) були опубліковані праці Гіппократа. Відтоді лікарі, які одержували ступінь доктора медицини на паризькому медичному факультеті, зобов'язані були давати «факультетську обіцянку», створену на основі «Канону», перед бюстом Гіппократа [474, с. 7]. У Франції закон зобов'язував лікарів на рівні з адвокатами, суддями, біржовими маклерами додержуватися професійної таємниці. Взаємини лікаря з хворим мали бути абсолютно довірчими, і саме тоді лікар міг допомогти хворому. У 1666 р. у Франції було прийнято декрет, що зобов'язував лікаря під загрозою штрафів повідомляти квартальних комісарів про всіх поранених, яким було надано медичну допомогу. Згодом лікар отримав право свідчити про туберкульоз (1893 р.) та аборт (1920 р.) [44].

У Німеччині лікар зобов'язувався повідомляти про венеричні хвороби (1927 р.), він мав свідчити про насильницьку смерть, тяжкі тілесні ушкодження й каліцтва. Лікарський статут Росії допускав розголошення лікарської таємниці щодо «прилипливих» захворювань і зобов'язував лікарів доводити до відома слідчих всі небезпечні поранення та пошкодження, які мають або можуть мати смертельні наслідки, та про отруєння [310].

У дореволюційній Росії лікарі після закінчення медичного факультету промовляли так звану «Факультетську обітницю», повний текст якої розміщувався на оборотній стороні диплома. У ній зазначалось таке: «Допомагаючи стражденним, обіцяю свято берегти довірені сімейні таємниці й не використовувати на зле їхню довіру». [69, с. 36–37]. Ставлення до збереження лікарської таємниці змінилося в 1920-х рр., коли прибічники скасування лікарської таємниці проголосили її пережитком буржуазної медицини. За повідомленнями газетних звітів, на одному з диспутів, що відбулися в Москві в 40 січні 1928 р., наркомздрав Н. Семашко так визначив ситуацію: «Держа твердый курс на уничтожение врачебной тайны – пережитка буржуазной медицины, каждый советский врач должен быть чутким общественным работником… Мы держим курс на полное уничтожение врачебной тайны. Это вытекает из нашего основного лозунга, что болезнь не

позор, а несчастье... Каждый врач должен сам решать вопрос о границах этой «тайны». Далі висловлена точка зору була підтримана, і тим самим питання було нібито вичерпано. Багато пізніше сам Н. Семашко визнав помилковість такої позиції Наркомздраву [502]. У Постанові ВУЦВК і РНК РРФСР «Про професійну роботу і права медичних працівників» 1924 р., а потім в Основах законодавства СРСР і союзних республік про охорону здоров'я, прийнятих Верховною Радою УРСР в 1969 р., лікарська таємниця встановлювалась тільки для лікаря.

Таким чином, історія виникнення лікарської таємниці свідчить про її перетворення з етичної норми на норму закону. Комерційна таємниця є одним з найдавніших способів охорони результатів інтелектуальної діяльності. Давні майстри зберігали секрети своєї професійної діяльності задовго до виникнення перших правових засобів охорони виключних прав. Ці секрети передавались з покоління у покоління, і ймовірно, першим захистом таких секретів виступала патріархальне суспільство, де батько мав владу над своїм сином, а господар над рабом. Правова охорона комерційній інформації надавалася ще в Давньому Римі, де законом передбачався подвійний штраф за примушення рабів розкривати секрети своїх господарів. Держави також приділяли особливу увагу охороні комерційно цінних ідей, навіть історично склався стереотип, що хоронителем таємниці виробництва фарфору, пороху, шовку є Китай; Сирія охороняла секрети виробництва дамаської сталі; Греція берегла секрет «грецького вогню», що використався під час морських боїв, та ін [272]. Однак не завжди мали місце законні способи суперництва, тому законодавство почало регулювати недобросовісну конкуренцію. Одним із видів правопорушень, визнаних недобросовісною конкуренцією, є неправомірний збір, розголошення та використання комерційної таємниці. Свобода заняття промисловою діяльністю, що одержала найсильніший розвиток наприкінці XVIII та XIX століть, і пов'язане з нею стрімке зростання економіки призвели до виникнення в конкуренції численних недобросовісних махінацій і методів, які швидко

перетворилися на загальну проблему, для вирішення якої необхідне було створення особливого механізму правової охорони [293].

1.3. Сучасні теорії державного регулювання інформаційною безпекою

Сучасне розуміння комерційної таємниці почало розвиватись в Англії під час промислової революції. У США перше задокументоване судове рішення стосовно комерційної таємниці датується 1837 роком. У Російській Імперії на початку XX ст. Г.Ф. Шершенєвич розглядав крадіжку конфіденційної інформації як одну з форм недобросовісної конкуренції: «Проявом недобросовісної конкуренції визнається збір чужих комерційних таємниць, або підкуп службовців, або направлення підставних робітників» [116]. Поняття комерційної таємниці припинило існування з прийняттям радянською владою у 1917 р. Декрету «Про робітничий контроль».

У радянський період діяло правило про обов'язковість найширшого та безоплатного поширення кожного досягнення, отриманого на окремому підприємстві, про «обмін досвідом» на адміністративній основі. Ще в 1930 р. XVI з'їзд ВКП(б) передбачив необхідність боротьби із секретністю. Хоча, така відкритість обмежувалась сферою цивільного виробництва, а таємниця існувала і захищалась адміністративними заходами, хоча й не мала характеру правової категорії. Повернення інституту захисту комерційної таємниці до законодавства відбулось наприкінці існування радянської державності, у Законі СРСР «Про підприємства в СРСР» .

У Європі питаннями дотримання та збереження банківської таємниці вчені та державотворці переймалися ще досить давно. З виникненням перших банків постає питання про додержання банківської таємниці. Вважається, що в установчих документах «Банку св. Амброзіуса», який був заснований у Мілані 1593 р., міститься перша письмова згадка про банківську таємницю [313]. Для підтримки довіри до банків у власні державі у XVIII ст. король Пруссії Фрідріх

Великий видав указ, за яким особи, які вели банківські операції, були зобов'язані довічно зберігати таємницю про них [27]. 42 Швейцарські банкіри понад 300 років тому дбали про збереження інформації про банківські рахунки клієнтів. У 1713 р. на Великій Раді Женеви було ухвалено перший відомий закон, який обмежує право банкірів розголошувати інформацію про своїх клієнтів. У першій половині минулого століття секретність швейцарських банків досить активно почала користуватися попитом, коли багато європейських держав почали підвищувати податки, для виплати боргів після війни, а заможні європейців почали шукати шляхи сховати гроші. Оцінивши позитивний вплив, який подібна практика спричиняє на економіку держави, в 1934 р. у Швейцарії ухвалили закон, що змушував банкірів нести кримінальну відповідальність за розкриття фінансової інформації. Швейцарський Закон про банківську діяльність від 1934 р. був прийнятий після того, як Адольф Гітлер і нацистська партія прийшли до влади у Німеччині [467].

На території сучасної України розвиток інституту банківської таємниці розпочався із створенням Державного комерційного банку Росії у 1817 р.. Зокрема, у Статуті Державного комерційного банку було визначено, що кожний вкладник міг щодня (винятком були святкові дні) вимагати для ознайомлення Банківські книги для спостереження за станом свого рахунку. Разом із тим зазначалося, що ніхто у жодному разі не мав права вимагати для ознайомлення рахунки та перекази інших осіб. У даному акті було закріплено, що чиновники банку зобов'язуються зберігати у непорушній таємниці усі рахунки приватних осіб під страхом відсторонення від посади, яку вони обіймали [77]. Значного розвитку банківська таємниця набула з 1903 р. шляхом закріпленням даної категорії у Статуті Державного Банку Російської Імперії. Окремо встановлювалась відповідальність за розголошення банківської таємниці службовцями банку [92]. Після подій 1917 р. відбувся певний регрес у розвитку інституту банківської таємниці. Банківська система того часу існувала на принципах про повну непотрібність та, навіть, шкідливість будь-яких таємниць у сфері економічної діяльності, крім державних. Почалися втручання у

діяльність приватних банків, існування яких із часом було взагалі заборонено. Як зазначає Г. Б. Романовський, термін «банківська таємниця» в законодавстві СРСР не вживався, та в цьому й не було необхідності, оскільки грошові заощадження зберігалися в ощадних касах, які належали державі [38]. Лише наприкінці існування СРСР розпочалися процеси, пов'язані з реформуванням як політичної системи, так і економічної. Саме з цим періодом можна пов'язувати початок відродження інституту банківської таємниці. У зв'язку з обмеженим обсягом цієї роботи не можливо розкрити історію становлення всіх видів таємної інформації. Зокрема, не було розглянуто становлення таємниці слідства, адвокатської та нотаріальної таємниці, таємниці страхування та інших.

Сучасний період свідчить про найбільш інтенсивний розвиток засобів захисту інформації починається у зв'язку з масовою інформатизацією суспільства. Проте, наприкінці 20 ст. математично було доведено, що забезпечити повну безпеку інформації в системах її обробки неможливо [496]. Історія використання інформаційних впливів на людину. В різні періоди історичного розвитку людської цивілізації інтенсивність застосування інформаційного впливу, як і досконаліть його організації, дуже різнилися. Тому з метою дослідження цієї діяльності з точки зору її історичного розвитку, виявлення основних чинників, які так чи інакше впливали на цей розвиток, науковці умовно поділяють історію інформаційного протиборства на три основні періоди.

Перший період інформаційного протиборства охоплює античні часи, епоху Середньовіччя та частину Нового часу до XVIII ст. включно. Перші письмові згадки про інформаційний вплив на суспільство у Стародавньому Китаї. У вже згаданому Трактаті про мистецтво війни китайського полководця Сунь цзи [448] наводиться опис і яскраві приклади застосування прийомів і методів психологічного впливу, які давали змогу досягати перемоги без битв або з мінімальними втратами. Важливе місце, зокрема, відводиться дезінформуванню противника, психологічній обробці власних населення і

війська з метою досягнення єдності в суспільстві напередодні і під час війни, здійснення інформаційних диверсій для розладнання військових союзів ворожої держави з іншими державами тощо.

Подальший розвиток воєнного мистецтва незмінно супроводжувався удосконалюванням форм інформаційно-психологічного впливу. Так, тривалий час у війнах Стародавнього Китаю застосовувався такий самостійний прийом інформаційно-психологічного впливу, як проголошення справедливою війни зі свого боку і несправедливою - з боку противника. Як бачимо, цей спосіб не втратив актуальності й досі і активно використовується в сучасних умовах. На період греко-перських воєн припадають згадки про спроби використання театру, поезії, образотворчого мистецтва з метою політичної пропаганди, а також протидії цьому з боку політичних опонентів. Новий етап розвитку практики пропаганди мав місце в античному Римі [305], зокрема, написання тенденційних біографій з метою уславлення певних аристократичних родів, мемуарний та епістолярний жанри, стають популярними різноманітні легендарні версії з історії Риму та походження римського народу, освячення і обожнення особи імператора. Спеціального розгляду в аспекті порушеної проблеми заслуговує психологічне та ідейно-пропагандистське забезпечення церквою різних воєнних акцій, таких, як, наприклад, збройна відсіч поганським навалам гунів, аварів, вандалів, відвоювання християнських святинь під час хрестових походів, міжконфесійна боротьба та боротьба з єресями. Не менш активно використовували релігійний аспект мусульманські завойовники. Один з перших історичних прикладів масштабного застосування дезінформації у воєнних цілях пов'язаний із вторгненням монголів до Угорщини у 1241 р. Розбивши угорців та їхніх союзників на річці Шайо, монголи серед захоплених трофеїв знайшли королівську печатку. За наказом Батия грамотні полонені від імені короля Бели написали угорською мовою указ про припинення опору, копії якого, скріплені королівською печаткою, було розіслано в різні кінці країни [56] На початку XVI ст. в концепції державної влади, що висунув і обґрунтував Н. Макіавеллі у книзі «Державець» вперше сформулював основні принципи

ведення інформаційного протиборства в політичній сфері. Він висунув тезу про те, що політик повинен поєднувати в собі риси лева і лисиці. Володіючи якостями цих тварин, він буде здатний, з одного боку, діяти рішуче, із застосуванням сили, з 45 іншого - маніпулювати масами за допомогою хитрості, спритності, обману. Брехня на благо суспільства визнавалася допустимою і навіть необхідною, а в роботі з підданими - «насильство для тіла і брехня для душі».

Винайдення Й. Гутенбергом друкарського верстату кардинально змінило можливості поширення інформації, прискоривши швидкість тиражування та зменшивши ціну виготовлення книг. В окремих країнах Європи з'являється інформаційне публічне видання - газета, яка спочатку була рукописною, а з часом - друкованою. З цим пов’язують необмежені можливості, причому не лише у військовій, а практично в усіх сферах суспільної діяльності (політичній, економічній, культурній тощо). Перший випадок використання друкованих, а не рукописних листівок, зафіксований під час війни Нідерландів за незалежність від Іспанії в XVI ст. На території Фрісландії було надруковано кілька тисяч примірників звернення до населення, яке стало важливим елементом консолідуючої пропаганди в 1567 р. у війні проти військ герцога Альби та звільнення фламандців від іспанського панування [60]. У Запорізькій Січі та державі Б. Хмельницького також вироблені були власні форми захисту військово-політичної інформації, зокрема дезінформації. В спогадах польських урядовців про нього «одне думає, про інше пише», «наміри його жодним чином не можна зрозуміти» [48]. Другий період інформаційного протиборства починається з середини XVIII ст. і закінчується Другою світовою війною включно. Найбільш яскравими є діяльність пропагандистського апарату Наполеона Бонапарта і нацистського Третього Рейху. Наполеон активно використовує можливості поліцейського відомства у справі ідеологічно-психологічного впливу на населення і контролю за ним для збереження власної диктатури. Він був одним із перших можновладців Європи, хто дійсно оцінив роль преси у формуванні громадської думки. "Чотири газети зможуть заподіяти

ворогові більше шкоди, ніж стотисячна армія". Усвідомлюючи повною мірою силу вплив преси на формування громадської думки, Наполеон диференційовано підходив до діяльності органів друку усередині країни та за кордоном. У Франції він газет заборонив писати про внутрішню та зовнішню 46 політику і скоротив кількість газет з 73 до 13. А у кожній окупованій країні засновував офіційний друкований орган: «Тазетт де Мадрид», «Газетт де Берлін», «Журналь дю Капітоль» тощо, на сторінках яких широко використовувались методи замовчування і дезінформації [62]. На зламі XIX-XX ст. повстає науковий інтерес до феноменів впливу на людську свідомість, зокрема на свідомість мас. У 1879 р. у Лейпцигу за ініціативою вченого В. Вундта відкривається перша психологічна лабораторія. П'ятнадцять років по тому у Франції виходить "Psyhologie des foules" (Психологія натовпу) Г. Ле Бона, який заявив про прихід "ери натовпу". Принципово нові завдання ставилися в той же період ідеологами роботи з масовою свідомістю. Відбувається зародження того виду інформаційно-пропагандистської діяльності, який прийнято називати англійським словосполученням "паблік рилейшнз" (ПР). Основним завданням фахівців ПР стало створення досконалих комунікативних технологій, тобто таких варіантів організації подачі інформації суспільству, які зможуть гарантувати, або, принаймні, обіцяти досягнення програмованого ефекту, наприклад, перемоги свого кандидата на виборах, підвищення попиту на рекламований товар тощо. Реально ПР виник внаслідок індустріальної революції, коли монополісти відчули що для досягнення успіху недостатньо методів управління лише виробничою сферою. Творцями перших технологій ПР дослідники вважають А. Лі та Е. Бернейса. За допомогою методів ПР А. Лі вдалося не тільки уникнути негативних наслідків від страйку шахтарів на шахтах Дж. Рокфеллера, але й використати цю акцію протесту на користь власника, значно підвищивши його імідж як дбайливого хазяїна. Значного розмаху застосування технологій ПР набуло після закінчення Другої світової війни. У 1948 р. засновуються Інститут ПР у Великій Британії та Асоціація ПР у США. Основними напрямками застосування можливостей ПР є

галузь реклами та передвиборна боротьба, але поступово і в інших сферах суспільного та державного життя цей інститут впевнено завойовує позиції. Поява ПР, окрім всього сказаного, означала ще й привернення уваги вчених, підприємців і політиків до роботи з інформацією. Внаслідок цього 47 вдосконалилися комунікативні технології, що застосовувалися в зовнішньополітичній сфері, зокрема, у війні.

Характерною рисою інформаційно-пропагандистської діяльності в європейських країнах періоду Першої і Другої світових воєн стала її централізація. Так, в часи Другої світової війни, в Англії існувало Міністерство інформації та Департамент пропаганди на противника, у Франції - служба військової пропаганди зосереджувалася при 11-му відділі Генерального штабу, а також "Будинок преси" та неофіційна організація "Альянс Франсе". Хоча США приєдналися до бойових дій на завершальному етапі війни, проте пропагандистську роботу на її потреби здійснювали з широким розмахом. При штабі американської експедиційної армії в Європі функціонувала "Психологічна підсекція", яка, поряд з проведенням широкомасштабних операцій з розповсюдження листівок, займалась і розробленням соціально-психологічної методики вивчення моралі противника, а в США діяв спеціальний орган пропаганди - Комітет громадської інформації, який мав поділ на секції: новин, іншомовних газет, громадської освіти, кінофільмів, відносин з промисловцями, реклами і карикатур. Пропагандистські машини СРСР і нацистського Третього Рейху не лише масово творили нові методи пропаганди, але й використовували населення своїх країн як своєрідні полігони, на яких проходили випробування нові зразки інформаційної зброї. Ефективність радянської пропаганди було продемонстровано ще в ході громадянської війни. Вже у грудні 1917 р. при Народному Комісаріаті іноземних справ було створено відділ міжнародної революційної пропаганди, а при видавництві ВЦВК - військовий відділ друку літератури іноземними мовами. Комуністична партія пропаганду за значенням ставила на один рівень з організацією бойових дій. Успішною була політична пропаганда

комісарівпропагандисти Червоної Армії. Маніпулюючи емоціями та свідомістю населення, вони вирішували питання комплектування збройних сил, управління економікою, формування нової структури адміністрації. "Шляхом пропаганди й агітації ми відібрали у Антанти її війська" – цю фразу приписують Леніну [305, с. 64]. 48 Апарат радянської пропаганди та агітації був націлений на радянське населення, щоби перетворити його в покірну безлику масу. Для цього створено нова міфологія з новими "героями", "титанами", "гігантами" і епічними картинами боротьби як на традиційному, так і на трудовому фронті. Схожі методи використовували міфотворці і вожді мас Третього Рейху. Незначна різниця полягала, лише в їх більшій відвертості. Наприклад, з'їзд націонал-соціалістичної партії в Нюрнберзі в 1936 р. прикрашав плакат "Пропаганда допомогла нам прийти до влади. Пропаганда допоможе нам завоювати увесь світ". Процес централізації контролю над пропагандою призвів спочатку до створення міністерства пропаганди, а пізніше міністерства громадської освіти і пропаганди.

Характерною рисою фашистської пропагандистської діяльності було ґрунтовне використання наукових розробок у цій сфері. Активно використовувалися напрацювання з психології підсвідомого. Відповідаючи на питання, чому Гітлер не приваблює іноземців, К. Юнг зазначав: "... для будь-якого німця Гітлер є дзеркалом його підсвідомого, у якому не для німця, звичайно, нічого не відображається. Він рупор, настільки посилюючий неясний шепіт німецької душі, що його може почути вухо його підсвідомого". Розроблені німецькими пропагандистами прийоми впливу на маси, до сьогодні використовуються в політтехнологіях. Це передусім театралізовані партійні з'їзди, масові зустрічі на стадіонах, радіотрансляції виступів лідерів на масові аудиторії тощо. Але основною характеристикою фашистської інформаційної політики, безумовно, є інформаційний монополізм. На сучасному етапі наука має в розпорядженні такі теоретичні надбання, на базі яких здійснюється технологізація інформаційної боротьби, тобто відповідні державні і недержавні структури, що причетні до такої діяльності, здійснюють розробку і апробацію

нових інформаційних технологій, прийомів, методів здійснення психологічного впливу, технічних засобів необхідних для такої діяльності. Подібні зрушення не могли не відбитися на зростанні ефективності застосування інформаційних технологій, яке може призводити до кардинальних змін в суспільній, економічній, політичній та іншій сферах окремої країни, або ж у світовому масштабі. 49 З кінця 1940 до середини 1980-х рр., в епоху так званої холодної війни, протистояння двох супердержав - СРСР і США - спричинило подальше вдосконалення форм і методів пропаганди та психологічної війни. У 1970-х рр. остання інформаційна революція пов'язана з винаходом комп'ютера висунула на перший план нову галузь - інформаційну індустрію, яка пов'язана зі створенням технічних засобів, методів, технологій для нових знань. Стрімке зростання обсягів інформації й об'єктивна зміна умов психологічної діяльності людини в сучасному світі привели до перерозподілу питомої ваги даних про оточуючий світ, що надходять до індивіда за допомогою генетичних каналів і в результаті безпосереднього сприйняття дійсності, на користь даних, що отримуються ним із засобів масової інформації.

Сучасні можливості техніки в поєднанні з науковою та публіцистичною літературою і періодикою дозволяють ефективно впливати на розум, свідомість і психіку мільйонів людей. Інформація і пропаганда стали сьогодні настільки могутніми, що здатні впливати на появу, перебіг і кінцевий результат політичних подій, в т.ч. глобальних проблем миру і війни. Становлення інформаційних прав людини. На теренах континентальної Європи намагання виділити об’єкт правової охорони, який би відображав суспільну потребу в захисті «автономії» особи, призвів до формулювання теорії «прав особистості», тобто невідчужуваних природних прав, пов’язаних із людиною як біосоціальною істотою [125]. В. Осятинський стверджує, що особливість прав людини власне в тому, що не вимагає жодного обґрунтування. Належать вони кожній людині власне як людині, становлять немовби істотну частину буття людиною [313]. Гідність людини є нерозривно пов’язана з фактом буття людиною. На буття людиною не мають впливу між іншим такі риси як вік, стан

фізичного чи психічного здоров'я, інтелектуальний чи емоційний розвиток, освіченість тощо. Ніхто за жодних обставин не може бути позбавлений гідності [43] Гідність людини не може залежати також від громадянства як правового зв'язку з державою [42]. Зараз визнається, що гідність людини властива їй від природи, а не з будь-якого рішення влади, є основою прав людини, прав громадянина [28]. Творцями сучасної доктрини прав людини вважаються діячі Просвітництва, які розвинули її на основі античної теорії природних прав і теорії суспільного договору як джерела державної влади. Монтеск'є сформулював принцип поділу влади на законодавчу, виконавчу і судову, і в його роботі «Про Дух законів» [261] він підкреслив взаємозалежність між свободою і верховенством закону. Ж.-Ж. Руссо в роботі «Суспільний договір» [406] визначає суспільний договір як основу свободи і рівності, при цьому рівність розглядається ним як умова свободи. Метою договору є створення позитивного права і гарантування свободи і інших прав. Ідея свободи, яка займає центральну позицію в моральній філософії Е. Канта, повинна бути відображена в правовій свободі, на яку має право кожна людська істота в силу її людськості [22]. Ідеї просвітителів відкрили шлях для радикальних змін в реальності суспільного життя. Ще в кінці XVII століття були закріплені окремі громадянські свободи в Англії. Були окреслені права підданих корони, в тому числі окремі процесуальні гарантії і свободи осіб (Habeas Corpus Act, 1679) і Білль про права 1689). У другій половині XVIII ст.. після великих соціальних революцій: американської та французької, були проголошені епохальні документи, як Декларація незалежності (1776, США) і Декларації прав людини і громадянина (1789 і 1793, Франція).

Передісторія і зміст цих декларацій відображає дві західні традиції прав. У країнах без абсолютних монархій в новій історії люди мають права, які обмежують уряд. Конституція є вищим законом, писана або неписана, а не воля володаря або держави. У країнах з постабсолютізмом держава має повноваження, а суспільство – обов'язки. Закон розглядається як свого роду подарунок від держави [.28]. До сьогодні можемо бачити це в культурі

англійської мови, яка використовується в правотворчості. В американській традиції, як правило, використовується поняття народу (people) і уряд (goverment), що свідчить про те, що люди мають той же статус, що і держслужбовці. Незалежні суди захищають права громадянина, докладаючи зусиль для того, щоб уряд діяв в рамках конституційних повноважень. Уряд перебуває в підпорядкуванні суспільству, і якщо порушує права громадян, то має нести за це відповідальність. У законодавстві континентальної Європи поруч з терміном «народ», як правило, вживається «держава» (state) в різних формах – республіка (republic) або монархії (monarchy), що відображає стійкий характер держави як самого буття (один з буквальних переказів «state» – статус, становище, визначати, встановлювати.) Держава нібито «резервує» за собою монополію на управління суспільством - людьми. Перша концепція, обґрунтована в ідеях Д. Локка, підкреслює невід'ємні права особистості і таких «природних» соціальних груп, як сім'я або церква; органи державної влади просто зобов'язані їх поважати. Ця традиція взяла гору в XVII ст. в Англії, особливо в американських колоніях, які в XVIII ст., воювали з британською державою. Хоча Англія поступово відійшла від неї, все ще йдеться про англо-американську традицію. Варто відзначити, що в Сполучених Штатах ідея прав людини не завадила знищенню місцевого населення (індіанців) і рабовласництва. У той час на континенті переважає інша концепція. Держава вважається «гарантом спільного блага і відповідальною за забезпечення індивідуальних потреб» [63].

Суспільство держав зі стійкими патріархальними традиціями влади очікує «батьківської» турботи від Батьківщини, що передбачає більш широке розуміння суспільних обов'язків і обов'язків уряду. На державу покладається не тільки гарантування безпеки і захисту життя, свободи і власності, але також забезпечення, при необхідності, задоволення основних потреб людини [305]. Незважаючи на численні відмінності прототипами актів про права людини вважаються англійський Білль про права (1689), американська Декларація Незалежності (1776), і французька Декларація прав людини і громадянина

(1789). Але це ще не були «права людини» в сучасному розумінні, тільки правомочності, які надавалися окремим людям в рамках, визначених суспільством. XIX ст. відзначене апогеєм колоніалізму і зростанням капіталізму, з одного боку, і скасуванням смертної кари, антиімперіалізмом, робітничим рухом і початком руху за права жінок – з іншого. В середині століття був ініційований 52 міжнародний гуманітарний рух, в основному в результаті злочинів, вчинених в Конго. У 1863 був сформований Міжнародний комітет Червоного Хреста і ратифіковано низку міжнародних конвенцій, що обмежили довільне застосування сили під час збройного конфлікту. Також значення набувають права меншин, особливо після першої світової війни. У ряді договорів і двосторонніх угод в Європі гарантується захист життя і свободи для всіх жителів таких країн, як Австрія, Болгарія, Угорщина і т.д., а також рівні політичні і громадянські права для членів усіх меншин. Хоча ці інструменти виявилися неефективними, положення про захист меншин стали відправною точкою для ідеї кодифікації прав людини в міжнародному праві. Водночас, в цей же період сформульоване поняття «privacy», що стало прекурсором сучасного права на захист персональних даних. В 1890 р. американські юрист и С. Уоррен і Л. Брандейс визначили його як «the right to be alone». Першим прецедентом, створеним на основі наукових розробок «права бути залишеним у спокої», стало рішення Верховного Суду штату Джорджія у справі «Павєсіч vs. Нью Ігленд Лайф Іншуранс Ко.» (1905 р.) [401]. Задовольняючи позов чоловіка, зображеного без його згоди в рекламному оголошенні, суд визначив об’єкт і мету правового захисту таким чином: «Той, хто бажає жити життям відносного усамітнення, має право обрати час, місце та способи, у які він буде піддавати себе громадському спостереженню». А у справі Griswold vs. Connecticut суддя Верховного суду США Дуглас вивів «право на приватність» з перших п’яти поправок до Конституції США, визнавши, що ці поправки «охороняють різні аспекти недоторканності приватного життя», зазначивши: «правом на недоторканність приватного життя старше ніж Білль про права» [65].

Усвідомлення зміни ролі інформації у суспільстві відбувалось поступово і нерівномірно в географічній перспективі. У 1946 р. Генеральна Асамблея ООН ухвалила одну зі своїх найперших резолюцій, де зазначено: «Свобода інформації є фундаментальним правом людини і … критерієм для всіх свобод, яким присвячено Організацію Об'єднаних Націй» [410, с.8]. Проте, вперше на міжнародному рівні про право на інформацію було задекларовано в ст. 19 53 Загальної декларації прав людини. Так, Загальна Декларація прав людини визначила свободу шукати, одержувати і поширювати інформацію та ідеї складовою права кожної людини на свободу переконань і на вільне їх виявлення. Аналогічне закріплення право на інформацію одержало також в інших міжнародно-правових документах, Європейській Конвенції про захист прав людини і основних свобод (п. 1 ст. 10), Міжнародному Пакті про громадянські і політичні права 1966 р. (п. 2 ст. 19) та ін. На основі цього можна зробити висновок, що права на свободу інформації, свободу думки і слова належать до так званих прав «першого покоління» - громадянських і політичних прав, які від початку вважаються невід'ємною частиною людської особистості [210]. На етапі створення другого покоління прав людини принцип універсальності застосовувався з метою усунення розбіжностей. А. Бенуа, французький академік, політолог і журналіст, зазначає: «теорії прав людини, здається, мало властиве визнання культурного розмаїття з двох причин: по-перше, через фундаментальний індивідуалізм і вкрай абстрактну природу об'єкта, якому надаються права, подруге, через її тісний зв'язок із Західною культурою». Якщо припустимо, що ідеологія прав людини всупереч її західним коріння, по-справжньому універсальна, виникають труднощі на рівні термінології. Термін «право» в розумінні індивідуальної властивості особи в середньовіччі не існував в жодній європейській мові. Це означає, що тривалий час не існувало навіть слова для позначення прав осіб, які б належали їм в силу їх людськості. Цей факт, а оцінює А. Макінтайр, ставить під сумнів реальність і змістовну наповненість цих прав. В арабській, китайській, японській мовах, а також в івриті і хінді, терміни, використовувані для позначення прав людини не

передбачають їх універсальності – yukt і ucita (правильний), nyayata (справедливий), dharma (обов'язок), китайський – chuan і li – влада і інтереси, арабська haqq – закон, який перш за все означає істину [54]. Незважаючи на всі невідповідності, концепція XX ст. проклала шлях до прав «третього покоління», яким була потрібна нова роль держави. Концепція прав «третього покоління» визнає суверенітет держави над громадянами, в той же час доповнює його стандартами міжнародного права і міжнародної системою 54 забезпечення. Забігаючи вперед, Конвенція про захист прав людини і основних свобод та Хартія основних прав ЄС розширить права людини в географічному сенсі – за межі національних держав. Після вичерпання наявних національних засобів захисту, будь-який громадянин може індивідуально звернутися до Європейського суду з прав людини. У той же час, в системі ООН проти держави виступити може не громадянин, права якого були порушено, але інша держава. Численні історичні події свідчать про часте використання подвійних стандартів. Наприклад – один з творців ЗДПЛ Р. Кассін, який виступав за культурний релятивізм в колоніальних війнах, писав: «в відсталих колоніальних суспільствах права людини можуть поставити під загрозу громадський порядок» [52]. Оскільки, процесу розвитку ідеї прав людини властиві як кількісні, так і якісні зміни, то, безперечно, варто погодитись з думкою, що розширює колективні права людини (третє покоління) піднесення та поглиблення права на інформаційний простір світу, на надання різноманітних послуг, що ґрунтуються на інтелектуальних інформаційних технологіях (зокрема на новітніх технологіях досліджень) і технологіях зв'язку (глобальна мережа «Інтернет»), забезпечення інформаційних відносин усередині країни і за кордоном. До розвитку сучасних кібернетичних систем під простором поширення інформації розуміли атмосферу, стратосферу, космос, водні акваторії океанів і морів. Зараз розуміння інформаційного простору включає додатково кібернетичні та віртуальні системи

Під час холодної війни політики неохоче згадували про права людини. У кожної держави на те були свої причини. В СРСР панував в сталінський терор,

Китай будував комунізм, Сполучені Штати більше дбали про свій суверенітет. Що цікаво, Сполучені Штати не підтримували ідею індивідуальних прав людини на міжнародному рівні. Д. Ф. Даллес заявив, що США «не буде учасником жодного документа з прав людини, прийнятого Організацією Об'єднаних Націй» [59]. І тільки в 1966 р. стало можливим прийняття наступних актів з прав людини – Міжнародного пакту про громадянські і політичні права та Міжнародного пакту про економічні, соціальні і культурні права. З З цього часу, можемо говорити про політизацію прав людини. Більш того, після Конференції з 55 безпеки і співробітництва в Європі, права людини широкого визнання не лише в Європі набули, а й підтримку правозахисників в країнах Східного блоку. У заключному акті конференції була встановлено право «знати про свої права», яке можна вважати прекурсором інформаційних прав людини. Помилкою буде вважати, що існували тільки західні модифікації прав. Не вдаючись в подробиці, теоретики комуністичного табору пропонували власну «соціалістичну концепцію прав людини». Відкидаючи природне право і справедливість як джерело, вона ґрунтувалася на нормах позитивного права. Соціалісти проголошували взаємний зв'язок прав і зобов'язань. Кожному праву громадянина повинен відповідати обов'язок держави. Взаємозв'язок прав та обов'язків знаходимо також в соціальному вченні Католицької Церкви. Однак, згідно з цим вченням, її джерелом є природне право. [61] Персоналістична концепція (від лат. persona - особа) є головною в християнському персоналізмі [482] К. Войтила сформулював персоналістичну норму, яка визначає людську особу як цінність саму в собі, настільки цінну, що за жодних обставин не можна використовувати її як засіб для досягнення мети, оскільки це вона є самоціллю. Ця виняткова цінність обумовлює належне ставлення до кожної людської особистості [60]. З цієї точки зору в своєму навчанні Іван Павло II багаторазово підкреслює пріоритет особи перед суспільством, з чого слідує, що жодна людина не може бути ніколи використана як засіб, навіть задля добробуту і розвитку усієї спільноти (людства). Віросповідання пов'язане з дотриманням певних таїнств. І цікавим з точки зору захисту інформаційних прав людини є

таємниця сповіді. Сповідь, є одним із семи християнських таїнств, установлених самим Христом, про що і згадується в Євангеліях. Покаяння, як таїнство, відомо майже всім релігійним конфесіям. Покаяння – один з найважливіших обрядів християнської церкви. Полягає в усному визнанні гріхів перед священиком, завдяки чому вважається, що людина при каятті, яке йде від серця, одержує прощення через священика від Бога. Зрозуміло, що в поняття «гріх» входять такі дії, що і у світській державі підлягають кримінальному покаранню. Тому дуже часто людина, що сповідує свої гріхи перед священиком, визнаючи себе винною у злочині, залишається 56 недосяжною для правосуддя. «Західна католицька церква, виходячи з думок Хоми Аквінського і цілого ряду вчених-богословів, встановлює «печатку мовчання» – sigillum confessionis, безумовно забороняючи священикам виказувати будь-кому те, що він почув під час сповіді. XXI стаття IV Латеранського собору попереджає, що за порушення цього правила священика очікує довічне ув'язнення у монастирі «найсуворішого» ордена»[133]. Подібних правил дотримувалася і православна церква. Перший, хто зважився порушити таємницю сповіді в Росії, став Петро I, вирішивши використовувати довіру віруючого до священика в боротьбі проти своїх ворогів. Одночасно варто звернути увагу, що таємниця сповіді в переважній кількості країн світу не проголошується як суб'єктивне право. Чого не можна сказати про деякі інші види особистої інформації, наприклад персональні дані або таємниця листування та іншої кореспонденції. Так, науковці стверджують, що у інків вже до початку XVI століття існували поштові гінці, які, крім державних повідомлень, доставляли до столу царя свіжу рибу, фрукти та інші продукти. Як вказує Сьєса де Леон в «Хроніці Перу», у інків законами було передбачено збереження таємниці відомостей, що містяться в пересилаються: «І в такому строгому секреті вели свої справи ті, хто проживав на поштових станціях, що ні на прохання, ні під погрозами , ніколи вони не розповідали про те, що збиралися передати в повідомленні, нехай навіть повідомлення вже пішло далі [поштою]»[227]. Поняття таємниці листування з'являється в різні указах і

посадових інструкції починаючи з XVII століття і стає поширеною правовою нормою до XIX століття. Систематичні порушення таємниці зв'язку до цього часу сприймаються саме як порушення і причетні чиновники поштових відомств і чорних кабінетів змушені виправдовуватися перед громадською думкою і навіть перед начальством. Так виглядало пояснення з приводу скарг на відкриття листів московським поштамтом в 1791 [175]«... Я начинаю сомневаться, не распечатываются ли там [в Берлине] сии письма столь неискусным образом, ибо клеем подлеплять не есть способ, употребляемый в России. Хотя и после меня рижский почтмейстер свидетельствует письма, но я уверен, что он своё искусство 57 знает и не подаёт сомнения корреспондентам. Московский почт-директор И. Б. Пестель.» Право на таємницю листування (пізніше до листування додалися телефон, телеграф та інші види зв'язку) стали вважатись похідними від права на таємницю приватного життя («privacy» - приватність). Причини спеціального відокремлення поняття «персональні дані» із загальної маси різноманітних даних пов’язані з тим, що вони є одним з найбільш важливих, делікатних та вразливих атрибутів недоторканості приватного життя людини, що потребує захисту за допомогою юридичних та організаційних заходів [100]. Починаючи з кінця 60-х рр. XX століття на теренах Європи у багатьох країнах почали розроблятись національні закони стосовно регулювання питання автоматизованої обробки та захисту персональних даних. Так, В. Брижко виокремлює основні причини для руху в напрямі удосконалення нормативноправового упорядкування відносин у сфері захисту персональних даних, із яких виходять європейські та інші країни: усунення передумов та порушень прав людини на її персональні дані; розвиток е-комерції; гармонізація національних законодавств [64]. Поруч із захистом персональних даних на базі свободи інформації, принципу гласності, свободи слова та друку в другій половині XX ст. як окреме суб’єктивне право виокремлюється право на доступ до інформації. Історія цього права корінням сягає ще 1766 р., коли в Швеції було закріплено “права знати” у Декларації прав людини і громадянина 1789 р. [183]. Закон був суттєво послаблений після

перевороту Густава III у 1772 р., тим не менше, закладені ним принципи стали основою для принципів, закладених у XX ст. А рівень Швеції за ВВП і соціальними стандартами, а також культура підзвітності й прозорості є найкращим доказом важливості забезпечення права на доступ до інформації й, зокрема, доступу до публічної інформації. Проте, ідея конституційного закріплення права на доступ до інформації була відроджена лише в другій половині XX ст. Проголошення "права знати" у країнах Європи та Сполучених Штатах Америки – це наслідок становлення громадянського суспільства та 58 демократичних перетворень, а в країнах, які розвиваються, – це умова утвердження громадянського суспільства. На межі XX і XXI століть інформаційні ресурси стали визначальним фактором розвитку і більшість країн констатували початок нової епохи – інформаційного суспільства. У 2000 р. прийнята Окінавська хартія глобального інформаційного суспільства, у якій було закріплено, що «всі люди повсюдно, без винятку повинні мати можливість користуватися перевагами глобального інформаційного суспільства. Стійкість глобального інформаційного суспільства ґрунтується на стимулюючих розвиток людини демократичних цінностях, таких як, вільний обмін інформацією та знаннями, повага до особливостей інших людей» [287]. У той же час в інформаційному суспільстві руйнується традиційна ієрархічна система цінностей. Кардинально змінюється і трактування понять «людина» і «її особистість». Організаційним принципом культурного життя людини стає принцип трансформації. Свобода особистості стає гарантом її безпеки [259]. Таким чином, проблема прав людини вийшла далеко за межі окремої держави, а обсяг прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей – національної держави, а й розвитком людської цивілізації в цілому. В науковій думці відсутній однозначний підхід до визначення інформаційних прав людини. П. М. Сухорольський у дослідженні підкреслює, що, наприклад, в англомовних джерелах виділяються так звані цифрові права людини (digital rights), під якими розуміють сукупність загальновизнаних та інших прав людини у контексті

поширення нових цифрових технологій, зокрема інтернету [49]. Розробка «Декларації прав людини і правових норм в інформаційному суспільстві» [50] стала першою спробою визначення міжнародно-правових рамок в цій сфері. Декларація була розроблена Комітетом експертів Ради Європи з інформаційного суспільства. Значну увагу на форумі було присвячено розробці норм відповідальної поведінки в інформаційному суспільстві. Учасники Міжнародного форуму «Права людини в інформаційному суспільстві: відповідальна поведінка головних дійових осіб» ініційованого Радою Європи, 59 закликали уряди захищати всі права людини, які стосуються інформаційного суспільства, від свободи слова до приватності і копірайту, не забуваючи про завдання подолання інформаційної нерівності і про належне управління. На їхню думку, «цілковита повага свободи слова та інформації державними та недержавними інститутами є необхідною передумовою побудови вільного інформаційного суспільства для всіх, а інформаційно-комунікаційні технології не повинні використовуватися для обмеження цієї фундаментальної свободи» [6]. Інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід’ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. Так, в соціальній сфері виникла небезпека нового типу нерівності: реальна загроза «інформаційного розшарування», яка веде до потенційну загрозу формування інформаційної еліти суспільства. У духовно-культурній сфері суспільства небезпека застосування в протиправних цілях інформаційних технологій призвела до загрози маніпулювання людською свідомістю, психічної і соціальної дезадаптації людини. Дещо забігаючи наперед зазначимо, що небезпека заподіяння шкоди здоров'ю людини в результаті використання інформаційних технологій породила загрозу розвитку

нових видів захворювань. Військово-політична сфера життєдіяльності сучасного суспільства відрізняється низьким ступенем захисту інформації про особу людини, що міститься в державних системах і комп'ютерних мережах. Небезпека контролю над людиною, маніпулювання, поширення конфіденційної інформації ведуть до потенційної загрози інформаційного тоталітаризму. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Негативним ефектом застосування сучасних технологій у військово-політичній сфері стали все ширші можливості застосування інформаційної зброї. Тим не менш, на кожному з вищезгаданих етапів інформаційна безпека людини залишалась і залишається вторинним питанням.

Наукові дискусії в сфері інформаційної безпеки особливо актуалізувались в останні роки XX сторіччя. При чому, як вже зазначалось, сучасні методи дослідження базуються на різних світоглядних позиція щодо соціального світу і людини, по-різному також вирішують дослідницькі завдання, а також використовують різні стратегії досліджень. Первинно, до другої половини XX століття, інформаційна безпека розглядалась, насамперед, як інформаційна безпека держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід’ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також гостро повстало питання кібербезпеки у складі інформаційної безпеки. Тим не менш, на кожному з цих етапів інформаційна безпека людини залишалась вторинним питанням. Саме до такого висновку призвів аналіз наукових досліджень питань інформаційної безпеки. Дзьобань О.П. і Пилипчук В.Г. вважають, що ідеал безпечного життя – дотримання в міжнародних відносинах загальновизнаних норм справедливості – сягає до часів античності, а наукове обґрунтування проблем національної безпеки взагалі й інформаційних її аспектів зокрема, вбачають у творах Т.

Гоббса та І. Канта [140]. З багаточисельних досліджень, що містили філософське осмислення проблем безпеки, зокрема Локка, Маркса, Енгельса, Тойнбі, Расела, Ясперса та інших, хотілось би звернути увагу на концепцію, запропоновану А. Бергсоном, який поєднував [інформаційну] безпеку з розумінням закритого і відкритого суспільства, а також вбачав шлях до безпечного стану людства через 61 відмову від «штучних потреб», спричинених переважанням розвитку в останні століття «тіла» людства, а не його «душі» [42]. Концептуально погоджуємось з позицією, що «подальші адекватні реальній соціальній дійсності наукові розвідки в царині інформаційної безпеки без опори на класичну спадщину уявляються досить сумнівними» [116]. При цьому, ці автори окреслюють чотири аспекти, на які звертали увагу класики в своїх працях: (1) інформаційно-етичний – Августин Блажений, І. Кант, Р. Оуен, А. Бергсон, А. Швайцер); (2) зв'язок досягнення безпечного стану і господарської та економічної структури, а також колізії природного й громадянського станів особистості – Цицерон, Гоббс, Локк; (3) Договірні відносини між державами задля формування відповідних організаційно-правових передумов і утворення об’єднань держави – Гроцій, Сен-Сімон, Ясперс, Тойнбі; (4) соціальний характер небезпек, які можна усунути лише змінивши структуру суспільства – Еразм Ротердамський, Франк. Важливо, що теоретики інформаційного суспільства, також попереджали про врахування інформаційної безпеки як визначальної умови становлення нової інформаційної епохи – Й. Масуда, Ю. Хаяші, Д. Белл, О. Тофлер, М. Кастельс, З. Бжезиньский, М. Маклюен, В. Іноземцев, П. Друкер, Ф. Вебстер, Д. Барні, А. Пенті та інші. Інформації у всіх концепціях згаданих дослідників (незалежно від назви) надається телеологічний статус, це обумовлює онтологічний вимір інформаційної безпеки будь-якої соціальної системи сучасності, осьовою детермінантою якої є зростання впливу розвитку інформаційно-комунікативних технологій.

Таким чином, наприкінці XX століття правове забезпечення інформаційної безпеки інтегрується з групою інформаційних соціальних

відносин, що стрімко розвиваються, і формують на початку інститут у межах адміністративного права, а потім – комплексну галузь інформаційного права. Тому слід відзначити значну кількість вчених-правників, чиї дослідження інформаційної сфери розпочинались в межах адміністративного права і інших галузей правової науки, а згодом значної уваги в їх працях набули питання інформаційного права – зокрема, Арістова І.В., Брижко В.М., Бєляков К.І., Бєлєвцева В.В., Гуцалюк М.В., Калюжний Р.А., Кормич Б.А., Копан О.В., Копилов В.А., Логінов О.В. Новицький А.М, Настюк В.Я., Олійник О.В., Рассолов М.М., Тихомиров О.О., Цимбалюк В.С. та ін. Іншу групу дослідників становлять вчені, що починали дослідження в рамках інших галузей наук, як соціальних, так і технічних, проте на сьогодні їх напрацювання становлять інтегральну частину інформаційно-правової науки, зокрема, щодо питань інформаційної безпеки – К.І. Бєляков, О.А Баранов, О.Д. Довгань, О.П. Дзьобань, Д.В. Дубов, І.Б. Жиляєв, Д.В. Ланде, В.А. Ліпкан, А.І. Марущак, М.А. Ожеван, В. Остроухов, І.Н. Панарін, В.М. Петрик, Г.Г. Почепцов, В.Г.Пилипчук, Є.Д. Скулиш, М.П. Стрельбицький, В.М. Фурашев, М.Я Швець, В.І. Ярочкін та інші. Однією з перших українських наукових праць, предметом дослідження якої був державно-правовий механізм інформаційної безпеки як системне поняття, стала захищена у 2014 р. Кормичем Б.А. докторська дисертація «Організаційноправові основи політики інформаційної безпеки України» . В цій праці вперше комплексно було проаналізовано організаційно-правові засади процесу формування і реалізації політики інформаційної безпеки України, а також виявлено специфіку змісту, форм та методів забезпечення інформаційної безпеки людини, суспільства, держави. До правової бази інформаційної безпеки було віднесено норми декількох галузей права, насамперед: конституційного, адміністративного, інформаційного, але її головним системоутворюючим чинником виступають єдині концептуальні засади державної політики інформаційної безпеки. Окрім того, Кормич Б.А. визначав правовий статус людини як об’єкта інформаційної безпеки, що визначається її правами в галузі інформації. В 2004 р. було видано перший український

навчальний посібник з інформаційного права «Основи інформаційного права», де питанням інформаційної безпеки було присвячено окремий розділ – «Інформаційна безпека як об'єкт інформаційного права» [29]. Науковці прогнозували, що в майбутньому інформаційна безпека, у міру розвитку інформаційного суспільства, виокремиться з інформаційного права в окрему субінституцію подібно до права інтелектуальної власності, його провідних складових — авторського права та права промислової власності [29]. Важливо, що вже на цьому етапі фахівці звертали увагу на необхідність створення базового закону в галузі 63 інформаційного права – Інформаційного кодексу чи Кодексу України про інформацію. На цьому етапі становлення наукової та правової категорії «інформаційна безпека» ототожнення її із захистом інформації було досить поширеним явищем, а подекуди має місце і досі здебільшого в зарубіжній науковій літературі. Безперечно, правове регулювання захисту інформації є складовою інформаційної безпеки, проте не є їй тотожним. Адміністративно-правовому захисту інформаційної сфери було присвячено монографію Настюка В.Я. та Бєлєцева В.В. «Адміністративно-правовий захист інформації», де обґрунтовано, що «захист інформації за своїм змістом передбачає, з одного боку – нівелювання небезпеки, з іншого - підтримання стану захищеності життєво важливих інтересів людини суспільства, держави від різного роду викликів та загроз» [68].

Більш широко і комплексно питання адміністративно-правового забезпечення інформаційної безпеки України досліджує Олійник О.В. в монографії «Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України» [290]. Автор пропонує широке розуміння забезпечення інформаційної безпеки як здійснення комплексу системних превентивних заходів з надання гарантій захисту від негативних інформаційних впливів: життєво важливих інтересів особи, суспільства, держави, політичного, економічного, науково-технічного, гуманітарного, соціокультурного розвитку, підтримання оборони, державної та екологічної безпеки, системи державного управління на необхідному рівні; забезпечення

інформаційного суверенітету та безпечного розвитку національного інформаційного простору; від маніпулювання інформацією, дезінформування та впливів на свідомість, підсвідомість і психіку індивідів , суспільних груп, суспільства в цілому; своєчасність і адекватність заходів протидії та нейтралізації всього спектру негативних безпеко генних чинників, що можуть бути застостосовані проти України» [290]. В цьому аспекті одним із важливих завдань, які мають бути вирішені в цьому дослідженні є визначення місця інформаційної безпеки людини у системі забезпечення інформаційної безпеки та зв'язків між її об'єктами 64 і суб'єктами; виявлення методологічних проблем правового регулювання відносин щодо інформаційної безпеки людини; окреслення пріоритетних напрямів державної політики України у сфері інформаційної безпеки людини. Розділяючи думку Баранова О.А., що «рафінованих чистих суспільних відносин, які піддаються регулюванню нормами тільки однієї галузі права не існує» [30, с.119], зауважимо, що інформаційні правовідносини щодо інформаційної безпеки людини регулюються також іншими нормами права.

Водночас, необхідно зазначити, що результати дослідження теоретико-правових засад забезпечення інформаційної безпеки, здійсненого Максименко Ю.Є., містили низку цінних висновків, зокрема, на підставі аналізу 65 досвід Європейського Союзу у сфері забезпечення інформаційної безпеки, було визначено потенційні загрози інформаційній безпеці України, тенденції та перспективи нормативно-правового регулювання окремих аспектів інформаційної безпеки України.

Також серед головних проблем нормативно-правового забезпечення інформаційної безпеки України виокремлено: наявність численних нормативно-правових актів різної юридичної сили у цій сфері; закріплення важливих засад підзаконними нормативно-правовими актами; певна невідповідність чинній Конституції України; неузгодженість нормативноправових актів та наявність багатьох прогалин; неоднозначність та неузгодженість закріплених дефініцій і відсутність навіть базових з них; наявність значного масиву декларативних

положень без механізму їх правореалізації; наявність численних бланкетних норм права, що не призводять до очікуваного ефекту; наявність чисельних абстрактних, суб'єктивних понять, що потребують офіційного тлумачення чи чіткого визначення; низький рівень правореалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки України [248].

Як можемо бачити, значна кількість означених у 2007 р. проблем й досі залишається не вирішеною. Водночас, заслуговують на увагу проблеми реалізації права на інформацію, серед яких основними Політанський В.С. називає: (а) необхідність законодавчого регулювання відносин у галузі права на інформацію, що виникають при використанні глобальних інформаційно-комунікаційних мереж; (б) правове забезпечення надання відомостей органами публічної влади та місцевого самоврядування, які не відповідають дійсності; (в) порушення права на таємницю приватного життя; (г) несвоєчасне надання інформації чи навмисне приховування інформації; (д) поширення відомостей, які не відповідають дійсності, що ганьблять честь і гідність особи; (е) невиконання обов'язку органів державної влади інформувати про свою діяльність та про ухвалені рішення тощо [316]. Дискусійним залишається питання щодо методології наукових досліджень інформаційної безпеки. На початках методологічною основою інформаційного права щодо з'ясування нових соціальних явищ визначався цивілізаційний підхід [294]. Згідно такого бачення сучасна методологія наукових досліджень поряд з використанням перевірених часом традиційних методів і підходів потребує нових для усвідомлення складних соціальних процесів, які мають і культурологічноправову спрямованість. І пропонувалось інтегральне спрямування методології вивчення соціального буття — соціальна синергетика. Погоджуємось з думкою, що методологія інформаційно-правових досліджень має враховувати поліаспектність та комплексність предметної сфери, яка знаходиться на межі соціальних і технічних наук. Задля використання сучасних досягнень світової науки цінним вбачається використання трансдисциплінарної стратегії досліджень Іммануїла Валлерстейна [40]., що дозволяє виявляти

подібності та 67 зв’язки між явищами, і який був запропонований на Всесвітній конференція ЮНЕСКО з вищої освіти – 2009: "Нова динаміка вищої освіти і науки для соціальної зміни і розвитку", як один з основних способів дослідження складних багатофакторних проблем XXI століття.

В останні роки дослідження питань пов’язаних з інформаційною безпекою, в тому числі правового її забезпечення, особливо актуалізувалось, що має як позитивні, так і негативні наслідки для вітчизняної науки і українського суспільства. Зокрема, 3 березня 2016 р. на загальних зборах Національної академії правових наук України затверджено Пріоритетні напрями розвитку правової науки на 2016-2020 рр., які порівняно з попередніми роками мають більш прикладний характер. Зокрема, в напрямку правового забезпечення інформаційної сфери України визначено необхідність наукового розкриття таких тем як: “Актуальні проблеми забезпечення інформаційної безпеки України, як однієї із основних функцій держави”; “Правові засади захисту персональних даних, інформації з обмеженим доступом, технічного захисту інформації, протидії негативним інформаційним впливам та впливам інформаційних технологій на шкоду людині, суспільству та держави”; “Основи правової інформатики, системної інформатизації нормотворчої, правозастосовної й правоосвітньої діяльності, розвитку електронного державного управління”; “Проблеми впровадження й розвитку інформаційно-правових підсистем електронного парламенту та уряду, електронних систем і баз даних у галузі держави і права в контексті децентралізації влади в Україні”[444]. Слід звернути увагу, що до розробки правового забезпечення питань, які безпосередньо пов’язані з інформаційною безпекою людини, суспільства і держави, що раз більше долучаються громадські організації. Активність громадянського суспільства безперечно є свідченням розуміння проблеми фахівцями в фахових колах – правничих, освітніх, медійних та серед фахівців з безпеки. Проте, такі ініціативні групи зачасту не можуть забезпечити належного наукового осмислення; не володіють правничою, в тому числі нормотворчою, технікою; не спроможні врахувати всі ризики. Водночас,

фінансування за рахунок грантових коштів, в тому числі зарубіжних і міжнародних організацій, створює небезпеку нав'язування відповідної ідеологічної позиції певним громадським ініціативам [160].

Водночас, суперечливим залишається питання подальшого системного розвитку науки інформаційного права. В сучасних умовах становлення інформаційного суспільства, національного інформаційного простору та глобального інформаційного протиборства, стрімкого розвитку інноваційних технологій та інших напрямків інтелектуальної діяльності, актуалізується проблема розвитку правової науки та потреба виокремлення інформаційного права і права інтелектуальної власності в окрему наукову спеціальність [230].

В результаті аналізу доктринальних підходів було встановлено, що наукові підходи до категорії «безпека» і «інформаційна безпека» існують фактично в кожному суспільстві та на кожному історичному етапі існування людства, проте сучасне їх розуміння значною мірою залежить від занурення конкретного суспільства, людини і держави в реальність інформаційного суспільства. Саме в таких умовах проблематика інформаційної та кібернетичної безпеки набуває особливої ваги з метою встановлення балансу інтересів особи, суспільства, держави та міжнародного співтовариства. Зміст інформаційної безпеки людини було досліджено з огляду на гносеологічний аспект відображення предмета в теорії, який полягає в тому, що явища і процеси відображаються у свідомості людини не дзеркально - як результат споглядального сприйняття дійсності, а через призму практично- діяльного відношення людини до світу і до самої себе, власних потреб і інтересів. Таким чином, безпека є усвідомленим явищем для конкретного суб'єкта суспільних відносин. Виходячи з того, що безпека є усвідомлене явище, можна зробити висновок, що усвідомлення її необхідності обумовлює глибоке розуміння сутності проблем, що виникають, реальних загроз. Розкриваючи філософські проблеми безпеки як соціального явища, відзначаємо, що розуміння інформаційної безпеки і усвідомлення її необхідності відбувається і виражається як на чуттєвому (підсвідомому), так і на раціональному рівнях.

Оскільки самозбереження є здатністю і основною властивістю свідомості людини, то прагнення до безпеки, в тому числі інформаційної, є виразом розумності людини, проявом усвідомленого змісту її буття, її суспільного і морального сенсу. Безпека при такому підході виступає як невід'ємний атрибут існування. Автор власне підтримує цю позицію, що не слід пов'язувати існування безпеки як явища виключно зі своїм антиподом – небезпекою. В сучасній правовій науці виявлено наявність множини підходів до розуміння як загальної категорії «інформаційна безпека», так і родової категорії «інформаційна безпека людини».

При цьому поширеним є ототожнення інформаційної безпеки людини з її забезпеченням. Це, на нашу думку, є методологічною помилкою, оскільки забезпечення (щодо інформаційної безпеки людини) стосується більшою мірою заходів (технічних, організаційних, правових, кадрових тощо), а сама безпека – суб'єктивного переживання людиною, що відображає активний зміст її свідомості, яка здатна прогнозувати, передбачити і уявити небезпеки, а також своєчасно і адекватно на них відреагувати. На нашу думку, у самому загальному вигляді під інформаційною безпекою людини можна розуміти її здатність зберігати свої істотні властивості, і забезпечувати власне існування і розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Тобто, не слід обмежуватись розумінням її як «стану», а найбільш відповідним, на нашу думку, є комплексний підхід, згідно з яким інформаційна безпека визначається через її істотні риси, найбільш важливі основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем. Тому задля визначення категорії «інформаційна безпека людини» було досліджено її онтологічний, гносеологічний і логічний зміст. І встановлено, що онтологічне розуміння інформаційної безпеки опирається на ціннісному вимірі об'єкта безпеки, який виражається через потреби людини, а можливість їх реалізації в правовому полі закріплюється через її права і свободи. З огляду на вищезазначене, в цій праці взято до уваги історичні передумови захисту інформації, використання інформаційних впливів на людину в інтересах

держави та інших суб'єктів, а також зародження інформаційних прав людини, зокрема, права на захист персональних даних та доступ до публічної інформації.

Очевидно, цим переліком не вичерпується проблема, проте обмежений обсяг роботи і завдання дослідження обумовили саме такий вибір. В результаті проведеного аналізу встановлено, що інститут інформаційної безпеки людини в Україні і світі є наймолодшим, порівняно з інформаційною безпекою держави чи суспільства. Протягом багатьох тисячоліть інформаційна безпека розглядалась, насамперед, з перспективи інтересів держави. Згодом інтенсифікація процесів інформатизації в усіх сферах, а особливо, зростання значення технічного захисту інформації зумовило становлення правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ та організацій, а також окремих галузей господарства. Так, в соціальній сфері виникла небезпека нового типу нерівності: реальна загроза «інформаційного розшарування», яка веде до потенційної загрози використання інформаційною елітою суспільства новітніх засобів в політичній сфері, зокрема встановлення т.зв. «цифрової диктатури».

У духовно-культурній сфері суспільства небезпека застосування в протиправних цілях інформаційних технологій призвела до загрози маніпулювання людською свідомістю, психічної і соціальної дезінтеграції людини. Соціально-політична сфера життєдіяльності сучасного суспільства характеризується низьким ступенем захисту інформації про особу людини, що обумовлює потенційну загрозу інформаційного тоталітаризму. На межі тисячоліть гостро повстало питання про міжнародну інформаційну безпеку, а також кібербезпеку у складі інформаційної безпеки. Негативним ефектом застосування сучасних технологій у військовополітичній сфері стали все ширші можливості застосування інформаційної зброї.

Водночас, базовою цінністю кожного виду інформаційної безпеки, на нашу думку, є людина, оскільки кожна загроза інформаційній безпеці в той чи інакший спосіб спрямована на її права, свободи і законні інтереси, впливає на її

життя і можливість задоволення своїх потреб. Відзначимо також, що наукові дискусії щодо проблематики інформаційної безпеки особливо у інформаційнорозвинених країнах світу особливо актуалізувались в останні роки XX сторіччя. При чому, сучасні методи дослідження цього явища базуються на різних світоглядних позиціях, а отже, порізному вирішують дослідницькі завдання. Якщо говорити про Україну, то наукове осмислення проблематики інформаційної безпеки людини є в процесі становлення і відбувається як вторинне по відношенню до інформаційної безпеки держави. Визначені основні осередки правових досліджень в галузі інформаційної безпеки. Акцентується необхідність подальшого системного розвитку науки інформаційного права, в межах якої здійснюються правові дослідження інформаційної безпеки.

Таким чином, наукове осмислення, визначення і нормативне закріплення категорії «інформаційна безпека людини» (як зрештою і суспільства, і держави) є необхідною умовою для закладення належних правових основ. Визначеність логічного змісту інформаційної безпеки залежить від розвитку наукового пізнання, а також від розбудови механізму державного управління.

РОЗДІЛ 2.
ОЦІНКА ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СУСПІЛЬСТВІ

2.1. Аналіз організаційно-правового механізму державного регулювання становлення інформаційної безпеки в суспільстві

Появу титульної концепції інформаційного суспільства зазвичай пов'язують з іменами японських вчених Ю. Хаяші та Й. Масуди. Введення самого терміну «інформаційне суспільство» приписується Ю. Хаяші, професору Токійського технологічного інституту в 60-х рр. XX століття. Й. Масуда, в свою чергу, був учасником розробки практично всіх програм "японської" моделі інформаційного суспільства, зокрема таких, як "Японське інформаційне суспільство: теми і підходи" (1969 р.), "Контури політики сприяння інформатизації японського суспільства" (1969 р.), "План інформаційного суспільства" (1971 р.), "План створення інформаційного суспільства – національна мета до 2000 р." (1972 р.), а його праці "Комп'ютопія" (1966 р.), "Інформаційне суспільство як постіндустріальне суспільство" (1981 р.) та "Гіпотези щодо генезису "Гомо інтелідженс" (1985 р.) стали антологією інформаційного суспільства. Праці Й. Масуди певною мірою були утопічними, оскільки він описував мрію про «суспільство, в якому буде процвітати людське інтелектуальна творчість, а не матеріальне споживання, проте мали й практичну цінність. Так, в "Комп'ютопії" він вперше обґрунтував та узагальнив основні характеристики інформаційного суспільства, серед яких: глобалізм, вихід людства на космічний рівень свідомості; світовий симбіоз людства і природи; перехід до існування людства у глобальному інформаційному просторі. Окрім того, вчений сформулював принципи концепції "глобальної комп'ютопії", зокрема: прагнення і реалізація цінності часу; свобода ухвалення рішень і рівність сприятливих можливостей для всіх;

розквіт різноманітних вільних спільнот; синергетична взаємодія в суспільстві; функціональні об’єднання, вільні від надмірного контролю влади; відродження теологічного синергізму людства і Бога.

Поняття "інформаційне суспільство" набуло всесвітнього визнання після публікації книги І. Масуди “The Information Society as Post-industrial Society” [62], де він сформулював основи майбутнього суспільства: основою нового суспільства буде комп'ютерна технологія, яка покликана заміщати або посилювати розумову працю людини; інформаційна революція перетвориться в нову продуктивну силу суспільства; в новому суспільстві стане можливим масове виробництво когнітивної, систематизованої інформації, технології і знання; точкою насичення ринку стане «межа пізнаного»; зросте можливість співпраці, спільного вирішення проблем; провідною галуззю економіки стане інтелектуальне (наукомістке) виробництво; в інформаційному суспільстві основним суб'єктом соціальної активності стане «вільне співтовариство»; основною метою в новому суспільстві буде реалізація «цінності часу».

Як вже зазначалось, специфікою японської концепції було те, що вона не була суто теоретичною ідеєю, а була сформульована в аналітичних звітах, поданих до японського уряду декількома організаціями: Агентством економічного планування, Інститутом розробки використання комп’ютерів, Радою зі структури промисловості, і була обрана як перспективний напрямок розвитку держави. Передбачалось, що інформаційне суспільство, в якому процес комп’ютеризації дасть людям доступ до надійних джерел інформації, позбавить їх від рутинної роботи, забезпечить високий рівень автоматизації виробництва. При цьому зміниться і саме виробництво : продукт його стане більш «інформаційно містким», що означає збільшення частки інновацій, дизайну і маркетингу в його вартості; «…виробництво інформаційного продукту, а не продукту матеріального, буде рушійною силою освіти і розвитку суспільства»[23]. В сам же зміст категорії «інформаційне суспільство», насамперед, вкладались примат інформаційних цінностей над матеріальними; економічна цінність капіталу, втіленого у знаннях (Knowledge capital) вища, ніж

капіталу, втіленого у матеріальній формі. Масуда висунув концепцію, згідно з якою інформаційне суспільство буде безкласовим і безконфліктним. Він писав, що на відміну від індустріального суспільства, характерною цінністю якого є споживання товарів, інформаційне суспільство висуває як характерну цінність час. У зв'язку з цим зростає цінність культурного дозвілля. Він навіть приходить до висновку про трансформацію сутності особистості і появу нового типу людей: на зміну «Homo sapiens» приходить «Homo intelligens», так як саме інтелектуальна діяльність стає для людини основним типом діяльності «Homo inlelligens» будуватимуть нову цивілізацію, котра суттєво відрізнятиметься від цивілізації «Homo sapiens» - глобальна спільнота громадян, котрі сформують поліцентроване, комбіноване суспільство, схоже на живий організм, з розгалуженою мережею безпосереднього зв’язку, спроможного швидко і динамічно реагувати на зміну зовнішнього середовища[62].

Особливу цінність становлять думки Й. Масуди щодо потенційних небезпек нового типу суспільства. Він передбачав, що людство постало перед вибором між діаметрально протилежними моделями майбутнього: між "Комп’ютопією", тобто справді демократичним, правовим інформаційним суспільством, та "автоматизованою державою". Тобто він передбачав небезпеку «контрольованого суспільства» внаслідок того, що на початках комп’ютери використовувалися, в першу чергу, військовими та іншими урядовими структурами, зокрема – службами безпеки, внутрішніх справ тощо. Серед головних соціальних загроз він називав футурошоки у зв’язку з швидкими соціальними трансформаціями, дії терористів, а також зазіхання на індивідуальну самотність та кризи підконтрольності [61].

Проблему футурошоку (шок майбутнього) підіймає також в своїй однойменній праці американський письменник, соціолог і футуролог Е. Тоффлер, розуміючи під ними руйнівний стрес і дезорієнтацію, що викликані надто інтенсивними і значними змінами за короткий проміжок часу [66]. Інша праця Е.Тофлера «Третя хвиля» стала передумовою до концепції постіндустріального суспільства Данієля Бела, найбільш відомого

американського теоретика цієї концепції. Тофлер висунув ідею про три хвилі розвитку суспільства: перша хвиля — аграрне суспільство, друга хвиля — індустріальне суспільство, третя хвиля — постіндустріальне суспільство. Тофлер зазначав, що " нова цивілізація несе з собою нові сімейні стосунки, інші способи праці, любові та життя, нову економіку, нові політичні конфлікти, і, понад все, це – змінену свідомість"[57].

В 70-ті роки відбувається конвергенція двох майже одночасно створених концепцій: інформаційного суспільства і постіндустріалізму. Концепція професора соціології Гарвардського університету Д. Белла була сформульована у його роботі "Прихід постіндустріального суспільства"(1967), де було виокремлено низку такі риси постіндустріального суспільства, як перехід від індустріального суспільства до сервісного (обслуговуючого) суспільства; визначальне значення теоретичного знання для здійснення технологічних інновацій; «інтелектуальна технологія» у якості основного інструменту при прийнятті рішень. Особливої уваги заслуговує його бачення розвитку інфраструктури: «Кожне суспільство внутрішньо пов’язане різними каналами, що дозволяє його членам здійснювати матеріальний і духовний обмін. Організація, фінансування, підтримка і керування цими каналами, або інфраструктурою, звичайно знаходилися в компетенції уряду.

У своїх роботах М. Кастельс не використовує поняття «інформаційне суспільство», на його думку, всі суспільства використовували інформацію і тому були інформаційними. У трилогії «Інформаційна епоха: Економіка, суспільство і культура» М. Кастельс здійснює аналіз сучасних тенденцій, що приводять до формування основ суспільства, яке він називає «мережевим». Виходячи з постулату, що інформація за своєю природою є таким ресурсом, який легше за інших долає усілякі перешкоди і межі, він називає інформаційну еру епохою глобалізації, де мережеві структури стають водночас, і засобом і результатом глобалізації суспільства. «Саме мережі складають нову соціальну морфологію наших суспільств, а розповсюдження "мережевої" логіки значною

мірою позначається на ході і результаті процесів, пов'язаних з виробництвом, повсякденним життям, культурою і владою» [54].

Таким чином, влада структури виявляється сильнішою за структуру влади. Приналежність до тієї або іншої мережі, разом з динамікою розвитку одних мереж стосовно інших, виступає, за М. Кастельсом, як найважливіше джерело влади. М. Кастельс досліджує дві суперечливих тенденції - яким чином глобалізація підсилює інтеграцію людей, економічних і соціальних процесів; та як пов'язані з глобалізацією процеси фрагментації і дезінтеграції.

Важливо, що в умовах глобалізації ринків і капіталів змінюється роль національної держави, яка поступово втрачає реальні важелі управління. Інститути і організації громадянського суспільства, котрі будувалися навколо демократичної держави і соціального договору між працею і капіталом поступово втрачають своє значення в реальному житті людей. Основною суперечністю (і відповідно рушійною силою розвитку) нового суспільства, що формується, заснованого на мережевих структурах, є суперечність між глобалізацією світу й ідентичністю (самобутністю) конкретного співтовариства. М. Кастельс, спираючись на концепцію французького соціолога А. Турена, вводить поняття «Ідентичність опору» і «ідентичність, спрямована в майбутнє» [54]. Цей опір спрямований проти основної тенденції розвитку сучасного суспільства – глобалізації. М. Кастельс припускає можливість переходу окремих соціальних груп від ідентичності опору до ідентичності, спрямованої в майбутнє, і тим посприяти перетворенню суспільства загалом із одночасним збереженням цінностей опору інтересам глобальних потоків капіталу й інформації. Поширення логіки мережевих спільнот змінює способи виробництва продуктів, досвіду, культури, влади. На думку Кастельса, мережі стали базовими осередками сучасного суспільства. Кастельс надає великого значення співтовариствам і стверджує, що реальну владу мають саме вони, а не «глобалізовані міста». Простір потоків відіграє центральну роль в розумінні мережевого суспільства за Кастельсом.

Це мережі комунікацій з певними центрами, в яких спільноти перетинаються. Еліти в містах не прив'язані до певної місцевості, але прив'язані до простору потоків. В умовах становлення інформаційного суспільства інтернет виконує функцію інтеграції людства через витіснення безпосереднього людського спілкування штучними формами соціальної комунікації, що призводить до зміни повсякденної соціальної взаємодії індивідів і соціальних груп, опосередковане спілкування між якими здійснюється за допомогою мережі. Проте інтернет не є єдиною мережею. Мережі в концепції мережевого суспільства розглядаються в широкому значенні – комерційні, освітні, розвідувальна, релігійна, політичні, терористичні тощо. Мережеве суспільство нівелює колишні форми стратифікації, але творить нові. Наступне, на що звертав увагу Кастельс, інтерактивність. Мережа, реалізована з використанням інтернет-технологій, дозволяє вилучити вертикальні канали зв’язку і забезпечити полівекторний обмін інформацією і спільне ухвалення рішень. Результатом є поліпшення якості інформаційного обміну і досягнення взаєморозуміння між партнерами в процесі їхньої ділової співпраці. Цей принцип на сьогодні є передумовою ефективного функціонування системи державної влади, а також її взаємодії з органами місцевого самоврядування та інститутами громадянського суспільства.

Адже демократизація передбачає якісну інформаційну взаємодію і спільне ухвалення рішень в інтересах всього суспільства. Інтерактивність нерозривно пов’язана з орієнтацією на споживача. Сучасні потреби ринку складно задовольнити через стандартизоване масове виробництво. Завдання знайти оптимальне співвідношення між масовим виробництвом і виробництвом, орієнтованим на споживача розв’язується в багатьох системах через інтерактивну взаємодію, що персоналізується, із замовником в режимі онлайн. Цей підхід Кастельса органічно екстраполюється на політико-правову сферу. Нормотворчість та правозастосування вимагає не лише публічних обговорень на етапі підготовки проектів нормативних актів, а й оцінки

ефективності правового регулювання за умови участі інститутів громадянського суспільства, бізнес структур і інших зацікавлених мереж.

Знання не підлягають економічному відчуженню й водночас створюють новий тип соціальної нерівності, бо застосування знань потребує відповідного інтелектуального рівня. Характерною тенденцією сучасного виробництва є збільшення питомої ваги висококваліфікованих спеціалістів. Досліджуючи методологічні проблеми державного регулювання становлення суспільства знань, І. Арістова зазначає, що обґрунтованою є наукова позиція щодо існування декількох етапів розбудови інформаційного суспільства. Якщо виходити із того, що перший етап розвитку інформаційного суспільства переважно ґрунтується на досягненнях інформаційних технологій та технологій зв'язку, то наступний етап його розбудови повинний допускати більш широкі соціальні, етичні та політичні параметри — це нове суспільство знань. На її думку, в основі суспільства знання лежить можливість знаходити, виробляти, обробляти, перетворювати, поширювати та використовувати інформацію з метою отримання й застосування необхідних для людського розвитку знань. Це суспільство спирається на концепцію суспільства, яке сприяє розширенню прав і можливостей, що включає в себе поняття чисельності, інтеграції, солідарності та участі [16, с.5].

Вплив інформаційного суспільства на формування особистості є актуально темою різноманітних наукових досліджень. Відбувається помітна уніфікація масової свідомості, оскільки люди «споживають» одні й ті ж інформаційні продукти глобального характеру (новини, реклама, художні твори і т.д.), йде масова пропаганда способу життя, притаманного цивілізації технологічно 172розвинених країн. Особливо значним є вплив механізму «глобалізації масової свідомості» на дітей та молодь. Втрачається національна ідентичність, відбувається деградація мови, нівелюються морально-етичні принципи, що не може не впливати на правову свідомість. Поширення масової культури, неминучість зіткнення з віртуальною реальністю, в якій важко розрізнити ілюзію і дійсність, створюють не лише психологічні і культурні

проблеми, але й правові. Створюючи свій образ у віртуальному просторі, людина втрачає адекватне сприйняття реального світу, в тому числі правової дійсності [158, с.64].

Штучно «розмивається» межа правомірної і протиправної поведінки за рахунок інформаційно-психологічного впливу на індивідуальну і суспільну свідомість. Наприклад, факт крадіжки продуктів харчування в супермаркеті і крадіжка інформаційного продукту в мережі не сприймаються однозначно, хоча обидва за змістом є правопорушенням. І це досить «невинний» приклад. Окремої уваги заслуговує «забруднення» інформаційного середовища і проблема «інформаційного шуму». Це питання досліджувалось нами раніше [171], лише зазначимо, що за допомогою «шуму» навколо певних подій, що мають правове і соціальне значення в державі і суспільстві формується негативне ставлення до державних органів, зокрема силових структур, а як наслідок поширення правового нігілізму як масового явища. Ігнорування особливостей соціалізації особистості, зокрема, формування правової культури в інформаційному суспільстві призводить не лише до послаблення цілеспрямованого впливу на суспільне життя, розбалансування соціальних взаємозв'язків, а й руйнує основи життєдіяльності людини. У міру наростання обсягу інформації стає важче орієнтуватися в її змісті, убезпечувати себе від неякісної інформації, а також від її надлишку. Для людини має значення і якість, і кількість інформації, що потрапляє в її інформаційне середовище. За умови інформаційного перевантаження порушується структура інформаційного середовища людини. Людина не отримує необхідної інформації для оцінки ситуацій, у яких вона діє, тому що вона не встигає переробити всю інформацію та виділити те, що корисно для її адаптування до нових ситуацій. Це призводить до виникнення небезпек. Важлива інформація, від якої залежить безпека життєдіяльності людини, не потрапляє в зону її уваги та не переробляється, виникає інформаційна криза. Це, по суті, інформаційний голод при інформаційній надмірності. Така ситуація виникає внаслідок відсутності знань про закони та закономірності функціонування інформаційного

середовища. Система цінностей та оцінок формує так званий «інформаційний щит», який захищає інформаційне середовище людини від шкідливої і небажаної інформації. Небезпеки виникають насамперед тоді, коли людина не має надійного «інформаційного щита».

Таким чином, людина (в першу чергу діти і молодь) отримує уявлення про правову дійсність на основі інформації, що є в її інформаційному середовищі. Кількість, якість і можливості доступу до такої інформації, а також здатність її критично сприймати («інформаційний щит») значною мірою визначають можливості правової соціалізації особистості. Підтримуємо думку професора Арістової І.В.: «хоча інформація є дійсно інструментом знання, але сама по собі вона не є знанням. Інформація, яка виникла із бажання обмінюватися знаннями та зробила більш ефективною їх передачу, залишається лише формою знання, точною й стабілізованою, індексованою за часом та користувачем. Інформація, навіть якщо вона може бути “покращена”, не обов’язково має правильне усвідомлення.» [16, с.8]. Окрім того, слід звернути увагу, що в сучасних умовах соціалізація, і освіта як її складова, повинні бути безперервними процесами. Тому актуальним є питання не лише надання можливості доступу до правової інформації, а й створення умов для безперервної освіти з метою формування системи цінностей, що відповідає вимогам безпеки особистості і держави в умовах становлення інформаційного суспільства.

Суспільне буття та історія людства творяться є результатом діяльності конкретних індивідів. При цьому спосіб залучення людини в суспільноісторичний процес обумовлена культурою в широкому розумінні, тобто не тільки суб'єктивними прагненнями і свободою вибору, але й об'єктивними умовами матеріального виробництва, рівнем суспільного розвитку, в тому числі - рівнем свідомості. Отже, те, що має назву «соціальної детермінації», є фактором залежності людей від продуктів та результатів їх, власної діяльності [451, с.54]. Із сукупної діяльності індивідів розвиваються нові об'єктивні історичні обставини, які, у свою чергу, визначають наступний

розвиток людей. Тим самим, не існує закономірних тенденцій історії без діяльності людей. Люди знаходяться в залежності від об'єктивних умов і обставин життя, але разом із тим створюють і змінюють ці обставини. В умовах нової цивілізації основними факторами людської само детермінації стають не стільки соціально-економічні і технологічні чинники, скільки особистісні - свідомості, вільного вибору, соціально-культурних пріоритетів. Також зазнає змін система культурних цінностей, зростає розуміння цілісності і єдності людства, багатоваріантності і різноманітності культурного розвитку. Розвиваються нові типи соціальних зв'язків людей. Суб'єкти, тобто індивіди та соціальні спільноти, на основі власних інтересів та потреб визначають зміст суспільних відносин у всіх сферах суспільного життя та діяльності - матеріальноекономічній (виробничі, технологічні тощо); соціально-політичні (політичні, правові, національні тощо); духовно-культурні (моральні, релігійні, художньоестетичні, наукові відносини). Хоча такий розподіл певною мірою є умовний, адже всі сфери життєдіяльності є щільно поєднані і взаємообумовлені. Звернемо увагу на окремі аспекти змін в соціальному бутті людини у зв’язку зі становленням інформаційного суспільства. В інформаційному суспільстві геопростір не зникає, однак суттєво змінюється суспільно-географічне бачення людини. У нових умовах активність людини на протязі певного проміжку часу означає, що вона просторово “розпливається”. Завдяки динамічному розвитку світової економіки, комунікаційних систем і міжнародного туризму розвиток контактів між жителями різних регіонів здійснюється швидкими темпами, що сприяє появі нового й універсального міжнародного способу життя. Новий рівень соціальних відносин призводить особистість до усвідомлення існування нової віртуальної реальності, в якій істотно розширюються рамки її зіткнення зі світом. Багато видів діяльності, важливих для існування, знаходять зовсім нову форму, і слідом за цим, процеси задоволення потреб особистості можуть бути так само перенесені у віртуальну реальність. Внаслідок цього вже в цій вторинній реальності з’являються і нові потреби, які також вимагають задоволення. Внаслідок віддаленості,

знеособленості або анонімності комунікаційних процесів у віртуальному середовищі змінюється уявлення не тільки про структуру комунікаційного процесу, але і про характеристики суб’єктів комунікації. "Багатоманітність варіантів кожного аспекту життя робить вибір перманентним станом сучасного індивіда. У глобальній цивілізації ніщо не є наперед визначеним, і все підлягає обов'язковому вибору: місце проживання і громадянство, форма сім'ї і характер занять, предмети споживання і духовні цінності. Без вибору дається лише сама ситуація вибору"[41, с.409]. Виникає ситуація множинності життєвих стилів у межах подолання суперечностей між збереженням цілісності та різноманітністю.

Таким чином, ідентичність твориться як необхідність впорядковувати різноманітність. Постає проблема якісної характеристики альтернатив, які обумовлюють або можуть обумовити вибір. Критерії та запити вибору походять саме з індивідуальної ідентичності. Показовим моментом у контексті проблеми самоідентичності та вибору, який не можна оминути, є категорія, про яку свого часу говорили С. К'єркеґор, представники німецького романтизму, екзистенціалізму, а сьогодні на цьому акцентують увагу багато сучасних філософів, а саме - тип людини-філістера (обивателя, споживача). Основні ознаки такої свідомості - замкненість у собі, боязкість і небажання відповідальності за власні рішення, страх вибору, фрагментарність, корисливість, превалювання емпіричного чинника у житті, закритість до нового досвіду, нівелювання моральних цінностей. "З міщанинаобивателя з його традиційними чеснотами, культивованими поколіннями з часів середньовічних городян, як то гостинність, милосердя, толерантність, працелюбство, поміркованість, - які на сучасному етапі спрощуються й нівелюються, - міщанин перетворюється на "людину масової культури", обивателя, який пасивно "споживає"... товари, культуру, життя" [402, с.125].

Тому актуальність питання інформаційної безпеки людини визначається, насамперед, в контексті концепції природного права. При цьому природне право людини постає як усвідомлена нею можливість і необхідність жити, бути

вільною, щасливою та вимагати від держави й суспільства сприяння реалізації своїх прав у межах, визначених принципами співжиття соціуму. Вперше на міжнародному рівні про право на інформацію було задекларовано в ст. 19 Загальної декларації прав людини, що в принципі відтворено і в ст. 34 Конституції України.

Так Загальна Декларація прав людини визначила свободу шукати, одержувати і поширювати інформацію та ідеї (ст. 19) складовою права кожної людини на свободу переконань і на вільне їх виявлення. Аналогічне закріплення право на інформацію одержало також в інших міжнародно-правових документах. Серед них — Європейська Конвенція про захист прав людини і основних свобод (п. 1 ст. 10), Міжнародний Пакт про громадянські і політичні права 1966 р. (п. 2 ст. 19) та інші. На основі цього можна зробити висновок, що права на свободу інформації, свободу думки і слова належать до так званих прав «першого покоління» - громадянських і політичних права, які від початку вважалися і вважаються невід'ємною частиною людської особистості[209, с.94]. Хоча окремі науковців зазначають, що права і свободи людини в сфері інформаційних відносин можна віднести до третього покоління [507, с.48]. Оскільки, процесу розвитку ідеї прав людини властиві як кількісні, так і якісні зміни, то, безперечно, варто погодитись з думкою, що розширює колективні права людини (третє покоління) піднесення та поглиблення права на інформаційний простір світу, на надання різноманітних послуг, що ґрунтуються на інтелектуальних інформаційних технологіях (зокрема на новітніх технологіях досліджень) і технологіях зв'язку (глобальна мережа), забезпечення інформаційних відносин усередині країни і за кордоном. Третє покоління прав людини - колективні права народів (націй), тобто права всього людства, що ґрунтуються на солідарності людей, їх належності до якоїсь спільності (асоціації). Це право на мир, безпеку, незалежність (самовизначення народів), на здорове навколишнє природне середовище, на соціальний і економічний розвиток як людини, так і людства в цілому [435, с.64]. В сучасному глобалізованому світі інформаційні права людини неможливо розглядати

відокремлено від суспільства і держави. Слід враховувати, що інформаційний вплив, який здійснюється на суспільство та державу, опосередковано діє на кожну людину. Особистість людини є передумовою й продуктом існування суспільства, держави. Сучасна людина постійно перебуває під впливом інформації, що поширюється в просторі цілеспрямовано або довільно. До розвитку сучасних кібернетичних систем під простором поширення інформації розуміли атмосферу, стратосферу, космос, водні акваторії океанів і морів. Зараз розуміння інформаційного простору включає додатково кібернетичні та віртуальні системи [141]. Визначення інформаційно-правового статусу особи в суспільстві і державі вимагає закріплення достатнього обсягу інформаційних прав людини. В сучасній науковій думці відсутній однозначний підхід до визначення інформаційних прав людини. Тихомиров О.О. відзначає, відсутність однозначної відповіді на питання щодо співвідношення права на інформацію та інформаційних прав, але виокремлює дві наявні наукові позиції [462, с.105]. Згідно першої – «інформаційні права» ширше за змістом поняття і об'єднує як право на інформацію в сучасному нормативному його розумінні (право збирати, зберігати, використовувати і поширювати інформацію), так і право на свободу думки і слова, право на вільне вираження своїх поглядів і переконань тощо. Тобто інформаційні права і право на інформацію співвідносяться як ціле і часткове[185; 240]

Другій позиції характерне певне змістовне ототожнення права на інформацію та інформаційних прав, що ґрунтується на сучасному сприйнятті права на інформацію не як певним чином відокремленого особистого немайнового права фізичної особи, а крізь призму науки інформаційного права, як універсального конституційного права на інформацію, що містить у собі комплекс можливостей, які в сукупності і становлять так звані інформаційні права суб'єктів [252, с.56].

Водночас, сам науковець вважає недоцільною критику наведених підходів, або ж вибір одного з них за єдину наукову основу не має особливого сенсу, оскільки вони відображають різні етапи еволюції прав в інформаційній

сфері: перший – усвідомлення права на інформацію як певного особистого блага і наявну сьогодні його нормативно-правову концепцію, а другий – перспективи становлення комплексного правового інституту «права на інформацію», що охоплюватиме всі інформаційні права, зокрема й цивільні, пов’язані з інформацією [462, с. 106]. Вже згадувана російська теоретик інформаційного права Бачило І. зазначає, що для визначення статусу людини в галузі права на інформацію необхідно 182 встановити його точну юридичну характеристику, яка передбачає, принаймні, три складових: а) формально-правову, пов'язану з визнанням права в формі його позитивного юридичного оформлення в законі окремої держави і міжнародного співтовариства; б) сутнісну, пов'язану з нормативно закріпленим змістом даного права, що реалізується через певні повноваження і кореспондуючі йому правові обов'язки; в) процесуальну, яка регулює порядок реалізації права[34, с.189].

Марущак А.І. основою інформаційних прав людини визначає право на інформацію, яке включає право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. При цьому основою права на інформацію вважає право людини на доступ (отримання) до інформації, свободу вираження поглядів і переконань, свободу обміну інформацією включає до обсягу поняття “право на інформацію” [251, с.25].

При цьому визначає суб'єктивне право на інформацію як гарантовану державою можливість фізичних, юридичних осіб і держави (державних органів) вільно одержувати, використовувати, поширювати та зберігати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб [252, с.56]. Костецька Т. А. зазначає, що з огляду на те, що до основних структурних елементів права на інформацію Основний Закон включає низку правоможливостей: право збирати, право зберігати, право використовувати та право поширювати інформацію усно, письмово або в інший спосіб – на свій вибір, які, у свою чергу,

структуруються в інші численні інформаційні права, можна вважати, що назване право є комплексним [212, с.115]. П. Сухорольський у спеціальному дослідженні підкреслює, що, наприклад, в англомовних джерелах виділяються так звані цифрові права і свободи людини (digital rights and freedoms), під якими розуміють сукупність загальновизнаних та інших прав людини у контексті поширення нових цифрових технологій, зокрема інтернету.

В умовах становлення інформаційного суспільства невизначеність у правовій площині цієї межі прав і свобод людини призводить до виникнення нових проблем, які вимагають наукового дослідження. Розробка «Декларації прав людини і правових норм в інформаційному суспільстві» [559] Комітетом експертів Ради Європи з інформаційного суспільства стала першою спробою визначення правових рамок в цій сфері. Основна увага була присвячено розробці норм відповідальної поведінки в інформаційному суспільстві різних суб'єктів - уряд, приватні компанії, ЗМІ та неурядові організації. На їхню думку, «цілковита повага свободи слова та інформації державними та недержавними інститутами є необхідною передумовою побудови вільного інформаційного суспільства для всіх, а інформаційнокомунікаційні технології не повинні використовуватися для обмеження цієї фундаментальної свободи» [6]. Розділ «Права людини в інформаційному суспільстві» Декларації містить 8 пунктів: право на свободу вираження, інформації та комунікацій; право на повагу до приватного життя і таємниці листування; право на освіту і загальний доступ до інформаційних технологій; заборона рабства і примусової праці; право на неупереджений суд і заборону на позасудове переслідування; захист власності; право на вільні вибори; свобода зібрань [559]. Як можемо бачити – переважна більшість – це права, які вважалися базовими і до становлення інформаційного суспільства

Проаналізувавши доктринальні підходи, норми міжнародного права та національного законодавства, вважаємо, що слід розрізняти дві різні категорії: інформаційні права і свободи людини, а також права і свободи людини в інформаційному суспільстві. При чому перша категорія є складовою другої. Під

інформаційним правами і свободами розуміємо комплекс прав, похідних від свободи інформації, як фундаментального права людини. До них належать: 1) інформаційні права, що пов’язані з особою (особистістю)7 людини – право на захист персональних даних, право визначати конфіденційність інформації та розпоряджатися нею; 2) право власності на інформацію; 3)право на доступ до інформації – в широкому розумінні, тобто доступ до публічної, екологічної, правової, наукової та інших видів інформації, в тому числі необхідної для реалізації інших прав та свобод – політичних прав, право на освіту, право на безпечне для життя та здоров'я довкілля, трудових та інших прав; 4) свобода поширення інформації будь-яким законним способом, яка є необхідною умовою повноцінного життя людини в демократичній державі, а також існування самого громадянського суспільства, її реалізація пов’язана з свободою думки і слова, правом на вільне вираження своїх поглядів і переконань; 5) право на безпечне інформаційне середовище.

Зупинимось більш детально на кожній з названих категорій. 1) Інформаційні права, що пов’язані з особою (особистістю) людини, виокремлюються нами на основі природно-історичного обґрунтування прав людини. Згідно нього людина є соціальною істотою і володіння правами і свободами має не лише правове значення, але й соціальне. Позбавлення чи обмеження прав людини спричиняє неможливість для задоволення своїх потреб та інтересів. Насамперед, до цієї категорії нами віднесено права, що пов’язані з реалізацією особистої свободи та права на приватність. Реалізуючи право на свободу та право на особисту недоторканість, фізична особа одночасно реалізує і комплекс прав на інформацію [330, с. 87]. Право на 7 Різниця в застосуванні категорій «особа і «особистість» в праві та інших соціальних науках розглянута в розділі І. Йдеться про соціальну природу людини, особливості її взаємодії з іншими людьми, соціальними групами та суспільством в цілому. 189 особисту свободу означає відповідну міру можливої та юридично дозволеної поведінки громадянина розпорядитися собою, своїми вчинками та часом. О.В. Кохановська доповнює цей перелік інформацією [215]. Тихомиров О.О.,

характеризуючи «інформаційні права першого покоління», які визначають невідчужувані так звані «негативні свободи», відносить до них: право на ім'я, його зміну і використання; право на таємницю особистого життя; право на особисті папери та розпорядження ними; право на таємницю кореспонденції; права особи, пов'язані з фото-, кіно-, теле- та відеозйомкою; право на свободу літературної, художньої, наукової і технічної творчості [462, с.106].

А їх інформаційна природа полягає в необхідності: по-перше, збереження в таємниці певної інформації про життя людини; по-друге, забезпечення цілісності інформації, яка ідентифікує особу, та самостійного визначення ступеня своєї публічності; по-третє, гарантування можливостей вільної творчої діяльності, результати якої у разі їх оприлюднення поповнюють інформаційний простір, перетворюючись у певні загальнодоступні знання. Чинне законодавство України не містить категорії приватності. Право на приватність – right to privacy – належить до основних прав і свобод людини. Його історичні корні сягають праць Арістотеля про дві сфери життя: публічну ("поліс"), пов'язану з політичним життям, та приватну ("ойкос"), пов'язану з домашніми справами. Інформацію як об'єкт цивільних правовідносин розглядають у таких проявах: як особисте немайнове благо в комплексі благ, наведених у ст. 201 та Книзі другій ЦКУ; як результат інтелектуальної діяльності, тобто як об'єкт виключних прав, урегульованих у ст. 199 ЦКУ; як інформаційний продукт, ресурс, документ, тобто об'єкт, який може бути інформаційним товаром і предметом будь-яких правочинів, з урахуванням особливостей та специфіки його як особливого об'єкта [214] Якщо в першому розумінні інформація є невіддільним благом від самої особи носія, то два наступних дозволяють розглядати інформацію як товар, що може відчужуватись, хоча йому й притаманні певні особливості. Баранов О.А., аналізуючи українське законодавство, зауважує його суперечливість щодо визначення права власності на інформацію [26]. В редакції Закону «Про інформацію» в 2011 р. було скасовано категорію право власності на інформацію. Дехто з правників

потрактував це в такий спосіб, що інформація не може бути об'єктом право власності [213].

Категорично не погоджуємось з такою позицією, оскільки правомочності володіння, користування і розпоряджання є необхідною умовою реалізації інформаційних прав і інформаційної безпеки. Власниками інформації можуть бути її виробники, тобто власник інформаційного об'єкта (оригіналу документа, першотвору бази даних і т.п.), який створив інформацію, відображену в цьому об'єкті, власник інформації, що його набув на договірних умовах; а також власник - споживач інформації, тобто власник інформаційного об'єкта (тиражованої копії документа, масиву документів і т. п.), який придбав конкретний екземпляр тиражу з метою споживання інформації, що міститься в придбаному їм інформаційному об'єкті. І право власності кожного з них буде відрізнятися. Ще один аспект права власності на інформацію – як національне надбання, належним чином не відображений в чинному законодавстві. Згідно Закону «Про наукову і науково-технічну діяльність» До наукових об’єктів, що становлять національне надбання, можуть бути віднесені визначені інформаційні ресурси, зокрема, інформаційні фонди. Проте, на нашу думку, слушною є рекомендація ЮНЕСКО вважати публічну інформацію надбанням народу, адже вона створюється в інтересах суспільства і за кошти платників податків. Такий підхід обґрунтовує право на доступ до публічної інформації. З цією метою відповідна норма має знайти відображення в Основному Законі. Українське законодавство регулює право власності на інформацію нормами цивільного права і інформаційного права. Однак, питання права власності суттєво виходить за межі предмету цього дослідження. Тому називаючи його, автор не заглиблюється у його розгляд. Проте, при здійсненні дослідження автор зіткнувся з такими питаннями, що можуть становити предметне поле для подальшої наукової розвідки, зокрема, питання визначення вартості інформації, реалізації права власності на бази даних, охорони права інтелектуальної власності в умовах постійного вдосконалення інформаційних технологій. 3) Право на доступ до інформації у сучасній науці інформаційного права

визначається як одне з інформаційних прав, що передбачає право кожного вільно збирати інформацію і право отримувати її від осіб, які володіють цією інформацією на законних підставах [139, с.63-72]. В останнє десятиріччя право на доступ до інформації здебільшого інтерпретували під кутом доступу до публічної інформації. Безперечно воно є 196 важливим і відображає принцип транспарентності

. Принцип інформаційної відкритості є важливою умовою існування демократичного суспільства, виражається в доступності для громадян інформації, що становить суспільний інтерес або зачіпає особисті інтереси громадян; систематичному інформуванні громадян про передбачувані або прийняті рішення; здійсненні громадянами контролю за діяльністю державних органів, організацій і підприємств, громадських об'єднань, посадових осіб та прийнятих ними рішень, пов'язаних з дотриманням, охороною та захистом прав і законних інтересів громадян; створення умов для забезпечення громадян України наданням їм інформаційних послуг іноземного походження. Як зазначає Т. Мендел, головне значення для гарантування реалізації вільного потоку інформації та ідей має визнання принципу, що державні органи володіють інформацією не для себе, в інтересах суспільства та від його імені [624]. Зміст права на доступ до інформації є похідним від свободи вираження поглядів, передбаченої статтею 10 Конвенції Ради Європи про захист прав людини і основоположних свобод [329]. З аналізу практики Європейського суду з прав людини по застосуванню цієї норми можна зробити висновок, що право на свободу вираження поглядів включає такі складові: свободу дотримуватися своїх поглядів; свободу одержувати інформацію та ідеї; свободу передавати інформацію та ідеї. Щоби мати власні погляди та/або передавати інформацію та ідеї необхідно мати достатній обсяг інформації, що робить право одержувати інформацію та ідеї основоположним. Органи державної влади самі створюють значний масив інформації, отримують і зберігають великий обсяг даних від фізичних та юридичних осіб. Як правило, це важлива інформація, що впливає на життя усієї спільноти. Можливість кожної окремої людини

одержувати всю суттєву інформацію, що існує у суспільстві, напряму залежить від того, чи вчиняє держава активні дії, щоб опублікувати, оголосити чи надати на запит відомості, якими вона розпоряджається, тобто від державної інформаційної політики [329]. 8 Від лат. Transpareo – відкрите, видиме наскрізь, зрозуміле. 197 Згідно Закону «Про доступ до публічної інформації» забезпечення права на доступ до інформації здійснюється двома основними способами – шляхом систематичного та оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом; та шляхом надання інформації за запитами на інформацію. Відкриті дані (open data) засновані на ідеї про те, що деякі дані повинні бути вільно доступними для всіх, щоб вони використовувались та перевидавали за власним бажанням, без обмежень із авторських прав, патентів та інших механізмів контролю. Цілі відкритих даних подібні до інших "відкритих" рухів, таких як відкриті джерела, відкрите обладнання, відкритий контент, відкритий уряд та відкритий доступ. Філософія відкритих даних відома давно (наприклад, в науковій концепції Мертона), але термін "відкриті дані" останнім часом стає популярним завдяки поширенню інтернету та Всесвітньої павутини та, особливо, запуску урядових ініціатив щодо відкритих даних. Основні принципи розкриття даних: доступність, відсутність технологічних обмежень, цілісність, відсутність дискримінації осіб та груп, відсутність дискримінації областей і починань і ін. Так у США у 2009 р. створено ресурс Data.gov, який по суті став першим у світі державним ресурсом відкритих даних. Було також оприлюднено Директиву Відкритого Уряду США. В Європейському союзі існують як загальноєвропейські програми підтримки та розвитку відкритих даних (open-data.europa.eu/en/data/), так і на рівні окремих держав-членів (Наприклад, Франція data.gouv.fr/fr/, Німеччина govdata.de/, Італія it.ckan.net/, Польща insigos.mg.gov.pl/Glowna.aspx та ін.). Канада і США на сьогодні є країнамии-лідерами по публікаціям даних (опубліковано понад 100 тис. наборів), слідом за ними йдуть Великобританія,

Франція, Індія, Японія, Німеччина і Італія (від 10 до 15 тис. наборів)[653]. США, Канада, Великобританія і Австрія не проводять моніторинг цільової аудиторії. У США регулярно оновлюються форуми, і будь-яка людина може взяти участь в «житті» відкритих даних[657]. У Великобританії розвинений громадський контроль за витрачанням державних коштів, визначені пріоритетні набори та 198 конкретні кроки по їх розкриттю. Запити щодо розкриття державної інформації публікуються на окремому сайті – WhatDoTheyKnow

2.2. Особливості організаційно- правового механізму державного регулюванняв забезпеченні інформаційної безпеки окремих категорій осіб

. Запит на розкриття інформації передбачає, що користувач сам оцінює можливу користь від розкриття даних; в разі відсутності соціально-економічних ефектів від розкриття даних дані не публікуються. Capgemini Consulting в залежності від темпів реалізації принципів відкритості, визначив три групи країн. «Початківці»: Австрія, Марокко, Об'єднані Арабські Емірати, Саудівська Аравія, Естонія. «Група послідовників»: Бельгія, Гана, Данія, Гонконг, Ірландія, Іспанія, Італія, Кенія, Молдова, Нова Зеландія, Норвегія, Сінгапур, Чилі. «Законодавці моди»: Австралія, Великобританія, Канада, США, Франція. Класифікація проводилася на підставі трьох параметрів: доступність даних, державна політика в галузі відкритих даних і функціональні можливості централізованого порталу відкритих даних [653]. В Україні історія розвитку відкритих даних розпочинається після прийняття Закону «Про доступ до публічної інформації» [343], але реально ресурси запрацювали у 2015 р., після того як був прийнятий Закон «Про внесення змін до деяких законів України щодо доступу до публічної інформації в формі відкритих даних» [337] та Постанова Кабінету Міністрів України «Про затвердження Положення про

набори даних, що підлягають опублікуванню в формі відкритих даних» [354]. На підставі цих документів державні органи зобов'язані надавати публічну інформацію в формі відкритих даних і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних10 у визначених форматах, що дозволяють автоматизоване оброблення такої інформації електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. В тому ж 2015 р. було прийнято Закон «Про відкритість використання публічних коштів», що став правовою підставою оприлюднення інформації про використання публічних коштів функціонують на офіційному державному інформаційному порталі. 9 https://www.whatdotheyknow.com/ 10 http://www.data.gov.ua/ 199 Відповідно до частини першої статті 212-3 КУпАП неоприлюднення інформації, обов'язкове оприлюднення якої передбачено, зокрема, Законом України "Про доступ до публічної інформації", - тягне за собою накладення штрафу на посадових осіб від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян. Складати протоколи про адміністративні правопорушення за статтею 212-3 КУпАП мають право уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини або представники Уповноваженого Верховної Ради України з прав людини. Таким чином, особа може звернутись до Секретаріату Уповноваженого Верховної Ради України з прав людини щодо порушення розпорядниками інформації вимог оприлюднення публічної інформації у формі відкритих даних та складення протоколу про адміністративне правопорушення за частиною першою статті 212- 3 КУпАП. Порядок звернення до Уповноваженого з прав людини та його Секретаріату, зокрема й щодо складення протоколу про адміністративне правопорушення за статтею 212-3 КУпАП, передбачається статтею 17 Закону України "Про Уповноваженого Верховної Ради України з прав людини". Відповідальність за неоприлюднення відповідної публічної інформації у формі відкритих даних має покладатись на відповідальну особу з питань доступу до публічної інформації розпорядника інформації, яка відповідає за оприлюднення відповідної інформації згідно із

Законом України "Про доступ до публічної інформації". Станом на 2016 р. до Секретаріату Уповноваженого Верховної Ради України з прав людини не надходили скарги щодо порушення розпорядниками інформації вимог оприлюднення публічної інформації у формі відкритих даних [231].

Проект передбачає сервіс пошуку та візуалізації даних з відкритих джерел про використання державою бюджетних коштів. Основний акцент зроблено на простоті використання та представлення специфічної інформації з масивів великих даних. http://www.007.org.ua/ відкритих даних, неефективність системи моніторингу стану оприлюднення та оновлення наборів даних на держаних порталах, сумнівність санкції статті 212-3 КУпАП щодо покладення відповідальності на відповідальну особу з питань доступу до публічної інформації розпорядника інформації (як правило, це державний службовець, який виступає лише виконавцем і немає реальної можливості впливу). Окремим проблемним питанням є громадська думка про недоцільність та безглуздість використання відкритих даних в країні. Деякі пояснюють це історичними особливостями розвитку України і ще не сформованим у наших громадян усвідомленням всієї перспективності демократичних цінностей [231]. Що стосується відкритих даних, що не належать державі, то їх системне правове регулювання відсутнє. Відсутнє на рівні законодавства і визначення відкритих даних, порядок надання такого статусу і його зміст. На нашу думку, інформація (дані) є відкритою, якщо будь-хто має до нього вільний доступ, може вільно використовувати та ділитися нею. При врегулюванні питань відкритих даних важливим видається також нормативно застерегти можливість автору (творцю контенту) визначати заходи, необхідні для збереження походження й відкритості таких даних. Особливої уваги, на нашу думку, заслуговує врегулювання правового режиму відкритості науково-технічної інформації, творів культури і мистецтва, інформації про товари і послуги, а також екологічної інформації (якщо її розпорядником не є держава). Наступним способом реалізації права на доступ до інформації є отримання інформації на запит. Право запитувати та одержувати інформацію в органах влади було

визнано на рівні Ради Європи ще в 1979 р. в рекомендації Парламентської Асамблеї РЄ, де зазначалося, що парламентська демократія може належним чином функціонувати лише тоді, коли люди є повністю поінформовані; що громадськість повинна мати доступ до урядових документів; що така свобода інформації становить інструмент стримування корупції та розкрадання публічних коштів. У документі ПАРЄ йшлося про свободу інформації та систему свободи інформації, оскільки на той час "право на доступ" ще не було сформовано і утверджено. Принагідно слід зазначити, що "свобода інформації" відрізняється 201 від "права на доступ до інформації", оскільки перша передбачає негативний обов'язок держави не втручатися в інформаційний обмін між особами, тоді як друге – позитивний обов'язок держави забезпечити доступ активними діями, а не лише утриманням від втручання у свободу особи[90]. У Рекомендації Комітету Міністрів РЄ щодо доступу до інформації, яка була оновлена в 2002 р., наголошувалося, зокрема, на важливості в плюралістичному, демократичному суспільстві прозорості публічної адміністрації та доступності інформації з питань суспільного інтересу [90].

Зазначалося, що широкий доступ до офіційних документів:

1) дозволяє громадськості мати адекватне уявлення та сформувати критичну думку щодо стану суспільства, у якому воно живе, та щодо органів влади, які ним керують, заохочуючи при цьому поінформовану участь громадськості у спільних справах;

2) сприяє ефективності та дієвості адміністрації та допомагає підтримувати її доброчесність, уникаючи ризику корупції;

3) робить внесок в утвердження легітимності адміністрації як публічної служби та зміцнення суспільної довіри до органів публічної влади.

В Україні право на інформацію визнавалося ще Законом України «Про інформацію» [360] у редакції 1992 р.. У 2011 р. набули чинності Закон України «Про доступ до публічної інформації» та нова редакція Закону України «Про інформацію».

Закон «Про доступ до публічної інформації» визначив:

1) порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації;

2) гарантії та принципи забезпечення права на доступ до публічної інформації;

3) суб'єктів відповідних відносин, їх права та обов'язки тощо.

Нова редакція Закону «Про інформацію» передбачає «право кожного на інформацію», визначивши при цьому одним із основних напрямів державної інформаційної політики «забезпечення доступу кожного до інформації». Крім того, Закон «Про інформацію» у статті 20 закріпив важливий принцип максимальної відкритості, згідно з яким «будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом» Законом врегульовано яка саме інформація може запитуватись, та які обмеження щодо доступу існують. Так, запит на інформацію – це прохання особи 202 до розпорядника інформації надати публічну інформацію, що знаходиться в його володінні (наприклад, інформація щодо використання бюджетних коштів або копія рішення сесії міської ради). Тобто йдеться про вже існуючу інформацію, якою володіє розпорядник.

Для відповіді на інформаційний запит розпорядник не повинен створювати нову інформацію.

Доступ до публічної інформації може бути обмежений, якщо вона є інформацією з обмеженим доступом:

1) конфіденційна інформація;

2) таємна інформація;

3) службова інформація.

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для

запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Таким чином, в законодавстві України знайшов відображення трискладовий тест, що є юридичною конструкцією – засобом для перевірки наявності необхідних умов для обмеження доступу до інформації. Це ті умови, виконання яких є обов'язковим для того, щоб виняток з відкритості інформації був правомірним. Іншими словами – обмеження доступу до публічної інформації без застосування трискладового тесту є незаконним і порушує право особи на інформацію. Будь-якому обмеженню доступу до інформації з боку розпорядника повинно передувати застосування «трискладового тесту» [90].

До 2015 р. органом, що контролював виконання норм щодо забезпечення права на доступ до публічної інформації була прокуратура, від 2015 і до сьогодні - це Уповноважений Верховної Ради України з прав людини. Рішення, дії чи бездіяльність розпорядників інформації також можуть бути оскаржені до керівника розпорядника, вищого органу або суду.

Запитувач має право оскаржити:

1) відмову в задоволенні запиту на інформацію;

2) відстрочку задоволення запиту на інформацію;

3) ненадання відповіді на запит на інформацію;

4) надання недостовірної або неповної інформації;

5) несвоєчасне надання інформації;

6) невиконання розпорядниками обов’язку оприлюднювати інформацію відповідно до статті 15 Закону «Про доступ до публічної інформації»;

7) інші рішення, дії чи бездіяльність розпорядників інформації, що порушили законні права та інтереси запитувача.

Практика свідчить, що державні службовці досить часто неправильно застосовують на практиці положення тесту, в результаті чого запитувачі не

можуть одержати суспільно важливу інформацію. Дані моніторингу виконання органами влади норм Закону «Про доступ до публічної інформації», який здійснюється Центром Політичних Студій та Аналітики з 2011 р., свідчать, що часто це відбувається через незнання чиновниками алгоритму його застосування. Водночас експертами Центру були зафіксовані непоодинокі випадки, коли чиновники зловживали і свідомо неправомірно застосовували тест для того, щоб не надати запитувану інформацію громадянам [90]. Водночас, аналіз звернень до Уповноваженого Верховної ради з прав людини та судової практики щодо порушення права на доступ до публічної інформації свідчить, що неправомірною може бути визнана відповідь розпорядника на запит, у якій він відмовляє в отриманні інформації: оскільки він не вважає себе розпорядником інформації в розумінні Закону України «Про доступ до публічної інформації»; якою він володіє, але з якихось причин вважає «непублічною» чи такою, що не повинна надаватись на запит; через порушення вимог законодавства щодо порядку оплати фактичних витрат на копіювання і друк; через вимогу вказати в запиті відомості, що не передбачені статтею 19 Закону України «Про доступ до публічної інформації»; якою він не володіє, але зобов'язаний відповідно до своєї компетенції; оскільки відповідає не по суті запиту; з будь-яких інших підстав, що не передбачені частиною першою ст. 22 Закону; оскільки запитувану інформацію можна отримати з офіційного веб-сайту чи інших загальнодоступних джерел; оскільки відповідає не по суті запиту; з порушенням встановлених законом вимог до відмови у задоволенні запиту на інформацію [524]. Серед типових порушень права на доступ до публічної інформації в Україні найбільш поширеними є порушення процедури (недотримання строків та форми), посилання до відкритих даних чи інформації, розміщеної на сайті (коли там відсутні відповідні дані); відмова з огляду на обмеженість доступу до такої інформації. Часто причинами таких порушень є перевантаженість та недостатній рівень обізнаності співробітників з питань права людини на доступ до інформації.

Належний рівень правової культури державних службовців, які беруть участь у нормотворчій діяльності, тлумачать та застосовують норми права, а також здійснюють юридичне інформування населення, є необхідною умовою гарантування дотримання прав і свобод людини, а також правового забезпечення розвитку демократичної правової держави. З питань доступу до публічної інформації заслуговує уваги значна активність громадянського суспільства. За останні роки неурядовими організаціями здійснюється постійна підтримка громадян щодо можливості реалізації цього права, а також захисту і відновлення порушених прав. Центр демократії та верховенства права заснував і активно підтримує Мережу захисників права на доступ до інформації, метою якої є гарантування правового захисту права кожного на доступ до інформації - було підготовлено, перекладено, опубліковано і поширено значна кількість практичних посібників, методичних рекомендацій та науково-практичних коментарів до законодавства, що стосуються прав доступу до публічної інформації, зокрема практичний посібник «Як оскаржити порушення права на доступ до публічної інформації?», Рекомендації розпорядникам публічної інформації, Науково-практичний коментар до Закону України "Про доступ до публічної інформації", навчальний посібник для державних службовців «Свобода інформації» тощо. У 2014 р. був запущений сайт «Доступ до Правди», що є уніфікованою платформа для надсилання електронних запитів розпорядникам інформації відповідно до Закону "Про доступ до публічної інформації", отже, для ефективного контролю громадян за діями влади. У 2015 р. Громадська організація «Центр UA» презентував його оновлену версію, що доповнена новим ресурсом, який дозволяє створювати новини і розслідування на основі відповідей на запити громадян. Таким чином, є всі підстави не погоджуватись з раніше згаданою позицією про «несформоване у громадян усвідомленням всієї перспективності демократичних цінностей». 4) Свобода поширення інформації будь-яким законним способом є нерозривно пов'язана з свободою вираження думок і поглядів, що є базовою для демократичного суспільства. Ця свобода значно ширша за відсутність цензури. Вона акумулює в

собі низку складових - свобода вираження думок і переконань, свобода слова, свобода друку, свобода ЗМІ; свобода журналістської діяльності; свобода творчості; свобода видавничої діяльності; право «виносити сміття з хати» («blow the whistle»)13, право мовчати та інші. Ця свобода закріплена як на найвищому міжнародному рівні (ст. 10 Конвенції про захист прав людини й основоположних свобод від 4 листопада 1950 р.), так і в Основному законі держави (ст. 34 Конституції України), посеред інших інформаційних прав. Водночас, цими ж нормами закріплено випадки обмеження цієї свободи (права – в українському законодавстві): ст. 10 Конвенції про захист прав людини й основоположних свобод: «Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду.»; ст. 34 Конституції України: «Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

Це право є «зворотною стороною» інших, в т.ч. інформаційних, прав – права на доступ до інформації, права на захист персональних даних та інших. Саме на межі цих прав і виникає значна кількість конфліктів. Рабіновіч П.М. зазначав, що в усі часи боротьба йшла не стільки за права, скільки за їх межі [394]. В умовах становлення інформаційного суспільства юридичне закріплення таких меж є визначальним для реалізації інформаційної безпеки людини. Новицька Н.Б. аналізуючи зловживання правом на свободу слова та інформації,

дійшла до висновку, що «зловживання правом свободи інформації може призвести до неефективності демократичного ладу, а саме стати причиною національної небезпеки, порушення громадського порядку, неконтрольованості суспільства владою, пропаганди насильницької зміни влади, закликів до національної, релігійної, регіональної, расової ворожнечі, нівелювання правом людини на приватне життя, загрозою її безпеки» [279, с.60-66]. Слід звернути увагу, що право на поширення інформації прислуговує не всім учасникам правовідносин у рівній мірі. Його обсяг залежить від суб'єкта інформаційних відносин (журналісти, адвокати, пересічні громадяни мають різні правомочності) і об'єкта (інформація з обмеженим доступом, інформація, що має суспільне значення, публічна інформація тощо). Важливою умовою реалізації права на свободу поширення інформації є захист прав осіб, що її поширюють, насамперед, журналісти. Поняття «свобода преси» охоплює не лише засоби масової інформації, як суб'єктів – юридичні особи, колективи людей. Цим поняттям охоплюється також індивідуальна свобода – можливість журналіста, який реалізує свій професійний обов'язок, і будь-якого іншого громадянина висловити свою думку в ЗМІ та прийняти участь в обговоренні суспільно важливих питань. В даному разі засоби масової інформації ефективно забезпечують свободу вираження поглядів будь-якої фізичної особи, тому обмеження свободи преси неодмінно обмежує індивідуальну свободу громадян, яка випливає зі ст. 10 Конвенції про захист прав людини й основоположних свобод та ст. 34 Конституції України [89].

Обмеження свободи преси, навіть з метою захисту репутації і прав інших суб'єктів, не безпідставно вважається опосередкованим обмеженням права громадян на отримання ідей та інформації. Це, в свою чергу, може обмежити можливості громадян приймати зважені та правильні рішення з питань життя суспільства, що завдає шкоди будь-якому демократичному суспільству. Як зазначає С. Шевчук, якщо «преса не може публікувати різні, навіть образливі, судження, люди позбавлені самостійного політичного вибору. А це означає, що

опозиція не має жодних шансів прийти до влади шляхом переконання виборців»[11].

ЗМІ безпосередньо займаються збором, обробкою та поширенням масової інформації. Можливість вільно збирати та поширювати інформацію, передбачає можливість вільно діяти без втручання інших осіб, зокрема держави, і без наявності в інших осіб певного кореспондуючого обов'язку. У справі „Бусуйок проти Молдови" Європейський суд висловлює таке тлумачення: «журналістська свобода включає також і можливість вдатися до певної міри перебільшення або навіть провокації»14 . Проте захисту при реалізації цієї свободи потребують і інші суб'єкти, зокрема, ті, які розкривають інформацію про зловживання. Набув значного розголосу приклад К. Ґан, яка працювала на посаді аналітика Головної комунікаційної штаб-квартири електронної організації прослуховування британського уряду. На початку 2003 р. вона одержала копію електронного листа з офіційними детальними планами США щодо прослуховування дипломатів країн-членів Ради Безпеки ООН. Великій Британії і США було конче потрібно отримати рішення Ради Безпеки, яка б санкціонувала заплановане ними вторгнення до Іраку. Ґан надала копію електронного листа до газети. Внаслідок цієї історії обидва уряди зазнали значних труднощів. Ґан визнала, що вона спричинила витік інформації і була обвинувачена в шпигунстві. У лютому 2004 р. обвинувачення проти неї було знято. Позиція полягала в тому, що британський 14 Зі справами ЄСПЛ, що розглянуті в роботі, можна ознайомитись на офіційному сайті http://www.echr.coe.int/ 208 уряд міг би зіштовхнутися з багатьма труднощами, якби він був зобов'язаний представити у суді конфіденційну юридичну консультацію, яку було використано для підтримки вторгнення до Іраку. У будь-якому випадку, у країні, де половина населення виступала проти війни в Іраку, здавалося малоймовірним, що присяжні визнають Ґан винною. К. Ґан не була захищена за британським правом. Вона втратила свою роботу і лише уникла кримінального вироку, оскільки уряд побоювався продовжувати її судове переслідування [411]. В українському законодавстві не існує механізмів

захисту таких осіб, а рівень ефективності судової системи не дозволяє сподіватись на судовий захист. Відсутній у українському законодавстві і принцип «Обсяг інформації, доступ до якої обмежується, про публічну особу має бути значно меншим, ніж обсяг інформації про приватну особу», який сформувався в практиці Європейського суду з прав людини.

Погоджуючись значною мірою з М. Кастельсом в твердженні, що кожне суспільство є інформаційним, очевидним є що значення інформаційних суспільних відносин в сучасному світі зросло не порівняно до жодної попередньої епохи. Фізичний і соціальний простір сучасності пов'язаний з інформаційним, і спостерігається тенденція все щільнішого їх поєднання. Таким чином, людина живе в багатовимірному середовищі, одним із важливих вимірів є власне інформаційний. Сьогодні вченими та фахівцями ставиться питання про необхідність розвитку інформаційної екології - науки, що вивчає закономірності впливу інформації на формування і функціонування людини, і людства в цілому, на здоров'я, як стан психічного, фізичного і соціального благополуччя, розробляються заходи щодо оздоровлення навколишнього інформаційного середовища. Необхідними складовими права на безпечне інформаційне середовище є як захист інформації, так і захист від негативних інформаційних впливів, яким більше уваги буде присвячено далі в цьому розділі, та в наступному – «Загрози інформаційній безпеці людини».

Однією з перших справ, в якій він знайшов відображення була справа «Лінгенс проти Австрії» від 08.06.1986 г. 209 Перелік означених питань не є вичерпним і потребує подальшого наукового осмислення та вдосконалення нормативно-правового і організаційного забезпечення права на доступ до інформації. Такий зміст інформаційних прав і свобод відображає доктринальний підхід. Обсяг і зміст правового, зокрема, конституційного, закріплення цих прав залежить від багатьох соціальних, в т.ч. політичних, правових та економічних, чинників: форми держави та її економічного розвитку, рівня демократизації суспільства; геополітичного становища; суб’єктів самих прав (обсяг прав громадян чи інших членів суспільства може

відрізнятися); зрештою, етапу становлення самого інформаційного суспільства, на якому перебуває держава. Правові норми, визначаючи конкретний зміст прав і свобод людини та громадянина, не дають їхнього вичерпного переліку. Водночас, однією з функцій права є прогностична, тобто визначає право покликано передбачати, а певною мірою і визначати, тенденції розвитку державно-правових явищ. Обсяг і зміст прав і свобод людини в сучасному суспільстві визначається не лише особливостями певного співтовариства людей, а й розвитком людської цивілізації в цілому. Також заслуговує на увагу твердження, що інформаційні права і свободи людини та громадянина становлять цілісний екзистенціальний феномен, який можна пізнати винятково крізь призму їх системних властивостей, що знаходить свій прояв у наявності прав і свобод інформаційного характеру у різних сферах життєдіяльності суспільства [44]. Відтак, систему інформаційних прав і свобод реалізуються в екологічній сфері, економічній сфері, політичній сфері, управлінській сфері тощо. В умовах становлення інформаційного суспільства кожні суспільні відносини переломлюються через інформаційну сферу. Друга категорія, права і свободи людини в інформаційному суспільстві, власне відображає зміни в змісті та способах реалізації, вже існуючих, загальноприйнятих та закріплених нормами міжнародного та національного законодавства права, суб’єктивних прав і свобод. Спробуємо звернути увагу на особливості реалізації окремих прав і свобод людини в умовах становлення чи розвитку інформаційного суспільства.

Для особистості головними системотворчими рисами є цілісність (тенденція до стійкості) та розвиток (тенденція до зміни). Внаслідок руйнування або перекручування цих рис особистість перестає існувати як соціальний суб'єкт. Це означає, що будь-який інформаційно-психологічний вплив на особистість має оцінюватися з позиції збереження чи руйнування її як цілого [416]. В інформаційному суспільстві, на кожному етапі його становлення і розвитку, інформаційно-психологічні впливи збільшуються і поглиблюються. А людська психіка має певні обмеження. Експериментально доведено, що

мозок звичайної людини здатен сприймати і безпомилково обробляти інформацію зі швидкістю не більше 25 біт на секунду (в одному слові середньої довжини міститься якраз 25 біт). При такій швидкості поглинання інформації людина за життя може прочитати не більше трьох тисяч книг, за умови, що буде щодня освоювати по 50 сторінок [59]. У той же час сьогодні лише у науковій сфері щорічно з'являється кілька мільйонів книг. Фахівці ввели визначення «макулатурного фактору» для літератури, яка користується нульовим попитом. Німецькі дослідники провели в одній із берлінських бібліотек вивчення попиту на 45 тисяч наукових і технічних видань, які зберігаються в ній. І з'ясувалося, що «макулатурний фактор» спрацював практично для 90 % книг [52]. Значна частина інформації, яка накопичується, швидко застаріває і вимагає заміни. Професійні знання в середньому застарівають за 3-4 роки (потребують оновлення) [416,с.76-88]. Тобто, на момент отримання диплому про вищу освіту, окремі знання з першого курсу навчання можуть бути неактуальними. Вперше над цим фактом замислились вчені у 70-х роках минулого століття. Тоді і з'явився термін «інформаційний вибух», який означав «лавиноподібне збільшення кількості публікацій у наукових журналах». З’явились прогнози кінця науки, оскільки вчений втрачає за таких умов відстежувати розвиток його галузі. Згодом термін «інформаційний вибух» почали розглядати під ще одним кутом – непотрібність переважної кількості накопичених людством знань для пересічної людини. 211 Крім того, виникає і питання якості, адже велика частина всієї людської інформації – нескінченне дублювання одного і того ж з незначними змінами. Особливої уваги заслуговує питання академічної доброчесності і плагіату. Однією з причин його появи є зростаюча кількість творців контенту. Інформаційне перевантаження «information overload» - термін, що описує труднощі розуміння проблеми і прийняття рішень, причиною якої є надлишок інформації.

Поняття згадується в книзі Б. Гросса «Управління організацією» [92] (1964 р.), але популяризував його Е. Тоффлер у своєму бестселері «Шок

майбутнього» (1970 р.) [656]. Термін і концепція передували виникнення мережі і становлення інформаційного суспільства. В останні роки термін "інформаційне перевантаження" модифікувався в «надлишок інформації» (information glut) та «смогу даних» (data smog). Термін, який раніше мав місце в межах когнітивної психології, перетворився в метафору широкого вжитку, яку використовують далеко поза академічними колами. Значним чином, поява інформаційних технологій посилила інформаційне перевантаження: інформаційні технології можуть стати основною причиною інформаційного перевантаження через їх здатність виробляти додаткову інформацію швидше і поширити цю інформацію до широкої аудиторії, ніж будьколи раніше . Інформаційне перевантаження має не лише психологічні, а й фінансові наслідки. За підрахунками Н. Зельдеса компанія Intel понесла майже в 1 мільярд доларів збитків через зниження ефективності роботи, у вигляді часу, витраченого на обробку непотрібних повідомлень електронної пошти і відновлення від інформаційних втручань. Дослідження Microsoft виявили, що для повернення до виконуваного завдання після перевірки електронної пошти пересічному працівнику необхідно в середньому 24 хвилини. Тобто, якщо говорити про прийдешню соціально-економічну формацію, з тотальними об’ємами різного характеру та сутності інформації, то сучасна людина, просто не готова до цього, її мозок ще не в змозі адекватно реагувати та опановувати такі масиви інформації. З цього приводу влучним є висловлювання наведене у Всесвітній доповіді ЮНЕСКО «До суспільства знань»: «В сучасних 212 інформаційних потоках, знайти необхідну інформацію, аналогічно до спроби напитись із пожежного крану – води виставить, але треба примудритись не захлинутися» [658]. Звісно, ІКТ фільтрують інформацію, проте, вони не можуть забезпечити рівня фільтрування яким володіє людський мозок. Надзвичайно важливими з точки зору гарантування інформаційної безпеки людини є володіння достатніми знаннями щодо власних прав і свобод, способів їх реалізації та захисту. Не можна оминути увагою, що в умовах існування відкритих, легкодоступних і легко наповнюваних інформаційних мереж існує

проблема дотримання прав і свобод людини в мережевому просторі, зокрема питання обмеження інформації, що вважається соціально чи/і економічно небезпечною, проблема безпеки персональних та інших видів даних, проблема.

дотримання авторських прав та прав виробників електронної інформації тощо. Заслуговує на увагу думка Городенко Л. М. щодо інформаційного розриву, що виникає щодо свободи поглядів, висловлювань та вільних трактувань [98]. Мережеві форми спілкування уможливили свободу висловлювань, наукового пошуку й творчої діяльності, а також гарантували і продовжують гарантувати можливість створення вільного комунікаційного поля, в якому відбувається обмін знаннями, проходять публічні дебати. Свобода висловлювань, властива мережевим комунікаційним формам, визначає зв'язки, що об'єднують індивідів у життєздатне товариство.

Позатериторіальний характер мережевих комунікацій сприяє поширенню будь-якої інформації, починаючи від пліток і закінчуючи засекреченими відомостями. В 1999 р. журналістами ВВС чи не вперше було вжито категорію «Cyber rights and cyber liberties», а також «digatal freedom»16, коли йшлося про необхідність змін в правовому регулюванню відповідно до технологічного розвитку, зокрема, спів розмірного захисту даних на фізичних носіях та в електронній формі [56]. Термін «кіберправо» прижився в англомовному середовищі (поруч з поняттям «кібербезпека») для означення галузі права, що регулює відносини, пов'язані з використанням інтернету, також комп'ютерів, програмного і апаратного забезпечення, інформаційних систем тощо. А термін 16 Кіберправа і кіберсвободи, цифрова свобода цифрових прав закріпився за означенням суб'єктивних можливостей людини щодо використання цифрових технологій. На сьогодні існує два основних підходи до розуміння категорії цифрових прав. Перший, цифрові права — це розширення і застосування універсальних прав людини до потреб суспільства, заснованого на інформації [66]. На користь такої позиції свідчить резолюція A/HRC/32/L.20 Генеральної Асамблеї ООН, яка підтверджує, що ті ж самі права, які людина має в офлайновому середовищі, повинні також захищатися в онлайновому

середовищі, зокрема, свобода вираження думок, яка може бути застосована незалежно від кордонів і в рамках будь-яких обраних людиною засобів масової інформації, відповідно до статей 19 Загальної декларації прав людини і Міжнародного пакту про громадянські і політичні права [317]. Ця норма фактично повторює визначену 6 грудня 2012 р. в Резолюції L13. У більш вузькому розумінні під цифровими правами розуміють права людини, які дозволяють отримувати доступ, використовувати, створювати та публікувати цифрові твори, або право доступу і використання комп'ютерів, інших електронних пристроїв або мереж зв'язку. І в одному, і в другому тлумачення одним із базових цифрових прав вважається право на доступ в інтернет.

Коли було підписано вище згадану резолюцію ГА ООН, такі країни, як Росія, Китай, Саудівська Аравія, Південна Африка та Індія, висловились проти. Вони, зокрема, вимагали вилучити з тексту фрагмент, у якому йдеться про “засудження заходів з обмеження та блокування доступу до розміщеної в мережі інформації” [504]. Серед положень цієї резолюції слід звернути увагу на заклики до всіх держав: «боротися з проблемами безпеки "таким чином, щоб забезпечити свободу та безпеку в інтернеті; забезпечити відповідальність за всі порушення прав людини та зловживання, вчинені проти осіб у зв’язку з реалізацією їх прав людини, визнавати, що конфіденційність в інтернеті є важливою; наголошувати на важливості освіти жінок та дівчат у відповідних технологічних галузях» [606]. В кількох країнах світу офіційно визнано право на доступ до інтернету (право на доступ до інформації в інтернеті) і / або заборонено державі 214 необґрунтовано обмежувати доступ людини до інформації та інтернету. В різний спосіб – шляхом визначення в законах, визнання рішенням Конституційного чи Верховного Суду це право закріплено у понад 10 країнах світу, наприклад, у Фінляндії, Естонії, Франції, Греції, Іспанії, Коста- Ріці. Була спроба закріпити на законодавчому рівні це право і в Україні. У 2014 р. було запропоновано внести зміни до Цивільного кодексу України, які б гарантували право фізичної особи на доступ до інтернету та встановлювали умови його обмеження [390]. Законопроект не був розглянутий

навіть в першому читанні. Слід розуміти, що право на доступ до інтернету не має на меті лише фізичну можливість доступу до мережі інтернет. Воно базується на комунікаційній цінності інтернету, що передбачає зв'язок цього права із іншими правами і свободами людини та необхідність доступу до інтернету для їх реалізації, зокрема, свободи думки, вираження поглядів та переконань, права на розвиток, політичних прав, екологічних та інших основних прав людини. Право людини завжди передбачає кореспондуючий обов'язок держави – забезпечити доступ до інтернету належної якості і відповідної ціни, а також не обмежувати без законних підстав доступ осіб до інтернету [60]. Тобто визнаючи це право людини держава зобов'язується створити відповідну інфраструктуру, забезпечити адекватність цінової політики на такі послуги, забезпечити рівні можливості доступу всім індивідам (незалежно від місця проживання, стану здоров'я, віку тощо), створити інші правові і організаційні гарантії реалізації цього права. Мукомела І.В. звертає увагу на ще один важливий аспект цього права - компетенцію населення, звертаючи увагу на її асиметрію в Україні [263].

Проте цифрові права не обмежуються правом на доступ до інтернету. Асоціацією прогресивних комунікацій17 ще у 2001 р. було розроблено Хартію інтернет прав. Хартія присвячена таким темам як: доступ в інтернет для всіх; свобода вираження думок і асоціацій (зібрань); доступ до знань; спільне навчання 17 Association for progressive communications - це, водночас, мережа і організація, членами якоъ на квітень 2017 р. було 51 членів-органызацій та 30 індивідуальних членів з 75 країн світу. Міссія APC: «Всі люди мають легкий та доступний доступ до безкоштовного та відкритого Інтернету для покращення свого життя та створення більш справедливого світу.» https://www.apc.org/ і творчість на основі вільного і відкритого програмного забезпечення і розробки технологій; недоторканність приватного життя, спостереження та шифрування; управління інтернетом; обізнаність, захист і реалізація прав. АПК заявляє, що "можливість обмінюватися інформацією і спілкуватися вільно використовуючи інтернет має життєво важливе значення для реалізації прав людини,

закріплених у Загальній декларації прав людини, Міжнародному пакті про економічні, соціальні і культурні права, Міжнародному пакті про громадянські і політичні права та Конвенції про ліквідацію всіх форм дискримінації щодо жінок [204]. К. Беккер, австрійський теоретик інформаційного антиглобалізму, вважає, що «основні цифрові права людини охоплюють право доступу до мережі, право вільно спілкуватися і висловлювати думки в мережі, і право на недоторканність приватної сфери». Водночас, він звертає увагу на те, що всі інформаційні і комунікаційні технології мають походження з військової промисловості і в сучасних умовах отримали розвиток в якості технологій «несмертельної зброї». Отримання доступу до цих засобів і контролю над ними зі сторони урядів, корпорацій та інших структур може становити загрозу. Тому реалізація цифрових прав людини покликана забезпечити кожному можливість безкоштовно і необмежено користуватися цими засобами і їх потенціалом. Питання обмеження доступу до інформації, в тому числі до інтернету, останні понад десять років постійно мають місце в судовій практиці розвинених країн світу. Прецедентом стало рішення ЄСПЛ, винесене на користь заявника у справі А. Йилдіріма проти Туреччини (Yildirim v. Turkey), де суд зазначив, що «інтернет став одним із основних засобів здійснення права на свободу вираження поглядів та свободи інформації». В Україні, після введення в дію Указом Президента Рішення РНБО України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [351], було розглянуто низку справ щодо порушення цим рішенням прав і свобод людини. Зокрема, у постанові Вищого адміністративного суду України від 14 червня 2017 р. по справі № 800/198/17 216 [322] щодо порушення права на свободу вираження поглядів у відповідності зі статтею 10 Конвенції про захист прав людини та основоположних свобод, а також порушення права позивача на свободу доступу до інформації, було відмовлено у задоволенні позову щодо визнання недійсними положень цього акту, які встановлювали заборону на певний період здійснювати надання послуг з доступу користувачам мережі до ресурсів певних російських сервісів. Серед аргументів суду має місце

посилання на Закон України “Про інформацію”, зокрема ч. 2 ст. 6, де визначено, що право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Ч. 2 ст. 7 цього Закону також передбачено, що ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом. Доступ до інтернет може бути обмежений в різний спосіб і з різною метою. Єдиною країною, де на законодавчому рівні заборонено доступ до інтернет є Китай. За результатами досліджень Комітету захисту журналістів18 та деяких інших досліджень обмежено доступ до мережі жителям таких країн як Туркменістан – інтернет недоступний для більшості громадян, підключення до мережі коштує в кілька разів більше середньої заробітної плати; єдиний сервіспровайдер - уряд, який, до того ж, блокує дуже багато сайтів, веде стеження за всіма обліковими записами своїх громадян в таких поштових сервісах, як Gmail, Yahoo, Hotmail і інші; сайти, що належать правозахисним організаціям (міжнародним або інших країн) блокуються, як і сайти великих інформаційних агентств; В'єтнам - влада цієї країни запитує інформацію в Yahoo, Google, Microsoft про громадян своєї країни, які працюють з сервісами вказаних компаній; урядом створено спеціальний орган для моніторингу роботи громадян своєї країни в інтернеті, в т.ч. розміщення контенту, спілкування по електронній пошті; 18 Комітет захисту журналістів (Committee to Protect Journalists (CPJ)) - міжнародна неурядова організація зі штаб-квартирою в Нью-Йорку, що займається захистом прав журналістів. блокуються сайти, які не влаштовують уряд; Туніс - провайдери зобов’язані звітувати перед урядом про громадян, які регулярно працюють в мереж; база блогерів, їх імен, паролів, адрес, особистих даних ведеться провайдерами і передається у відповідні урядові служби на регулярній основі; міжнародний трафік контролюється урядом; блокуються тисячі веб-

сайтів, які не влаштовують уряд; заборонені торренти і інші види файлообміну; Китай – має чи не найбільш розвинену програму по цензурі мережі у світі; провайдери зобов'язані блокувати сайти, які не бажані уряду, знищувати відповідний контент і вести контроль за поштовим трафіком; заборонені низка соцмереж; Іран – переслідується критика уряд або релігійних діячів,блогери зобов’язані реєструватись в Міністерстві мистецтва і культури; блокуються сайти, де критикується режим правління, а також особливо контролюються сайти організацій захисту прав жінок; Саудівська Аравія – урядом блокується сайти понад 400 тисяч сайтів політичної, соціальної і релігійної тематик; Куба - інтернет важкодоступний, поширеним є користування через урядові точки доступу, де ведеться моніторинг за кожним IP; фільтрується контент, перевіряється історія роботи в мережі; завантажувати контент в мережу дозволено обмеженому колу осіб, наприклад, блогерам і чиновникам, які підтримують режим; Бірма - інтернету практично немає, існуючі точки доступу дуже жорстко контролюються урядом, включаючи електронну пошту, блокуються сайти, де є хоча б найменша згадка про права людини; ті, що належать політичній опозиції (ці сайти розміщуються і наповнюються за межами Бірми); Північна Корея - доступ до мережі має близько 4% населення, серед яких в основному військові та чиновники; для інших існує «Кванмен» — внутрішня закрита мережа; блогінг заборонений, а весь завантажений контент перевіряється відповідними службами безпеки; Саудівська Аравія - цензурі піддається книговидання, ЗМІ і доступ в інтернет, ввесь інтернет-трафік в королівстві проходить через систему проксі-серверів, розташованих в науково-технологічному центрі імені короля Абдулазіза; в країні існує спеціальна Комісія з комунікацій та інформаційних технологій, яка здійснює блокування ресурсів, в т.ч. за персональними заявками громадян; Ефіопія – має низький % інтернет-користувачів - всього 4% населення країни; монополія держави на телеком-послуги, нерозвинена інфраструктура і політика заборони на розвиток телекомунікацій призвели до неадектваних цін, окрім того мережі повністю відсутні в сільській місцевості, де проживає 85% населення країни; присутня

цензура і переслідування за необережні висловлювання. Неможливо в межах однієї праці розглянути і проаналізувати так значний обсяг питань. Зокрема, поза увагою авторка свідомо залишила питання реалізації політичних прав в умовах е-демократії і засилля політтехнологій, заснованих на маніпуляції інформацією; співвідношення свободи слова і права на захист від шкідливої інформації; трудові права і соціальний захист в умовах віддаленої праці та фрілансерства; свободи совісті і права на національну самоідентифікацію в умовах глобального інформаційного простору та багато інших.

2.3. Особливості правового забезпечення державного регулювання інформаційної безпеки

Оскільки інформаційна безпека людини базується не лише на її захищеності від інформаційних загроз, але й передбачає можливість людини як біологічного організму і соціальної істоти функціонувати, розвиватись і досягати бажаних для себе результатів в інформаційному суспільстві. Сучасні міжнародно-правові акти передбачають обов'язок держав створити рівні можливості для захисту своїх прав онлайн в тій самій мірі, що і в реальному просторі. Комітет Міністрів Ради Європи в Рекомендації CM/Rec (2014)6 [397] зазначає, що існуючі права людини та основні свободи в рівній мірі відносяться як до оффлайн, так і до онлайн простору. Ніхто не повинен бути об'єктом незаконного втручання в здійснення прав людини та основних свобод під час перебування в інтернеті. Швидкі темпи поширення і популярність інтернету пояснюються світоглядними установками інформаційного суспільства. Інтернет відповідає ціннісним очікуванням сучасної людини: доступність, необмеженість, варіативність, тиражування, оперативність. При цьому різні категорії осіб знаходяться у неоднакових умовах щодо можливості реалізації своїх прав і свобод в інформаційній сфері, зокрема, відрізняється ступінь захищеності в інформаційному суспільстві, види і інтенсивність небезпек, що

їм загрожують. Серед об’єктів інформаційної безпеки можна виокремити категорії, що характеризуються наявністю спільних інформаційних загроз їх безпеці і необхідністю особливого правового забезпечення. Зокрема, в цьому дослідженні спробуємо звернути увагу на наступні:

1) окремі вікові групи: насамперед, діти, підлітки і молодь, а також люди похилого віку;

2) люди з обмеженими фізичними можливостями, особливостями інтелектуального розвитку та психічними порушеннями,

3) люди, що здійснюють діяльність, яка має або може мати важливі соціальні наслідки – державні службовці, медійні особи та журналісти, правозахисники, громадські активісти і політичні діячі тощо;

4) населення окремих регіонів країни чи населених пунктів, що володіє специфічними соціокультурними особливостями, в т.ч. релігійними, етнічними, мовними, демографічними;

5) люди, що пов’язані з військовими діями на сході України – військовослужбовці, їх сім’ї, а також сім’ї загиблих, населення окупованих територій, «сірої» зони, внутрішньо переміщені особи тощо.

Цей перелік не є вичерпним, його метою є окреслення межі предмету дослідження. Діти, підлітки і молодь. За даними досліджень 2011 р. в США близько 80% дітей у віці до 5 років користувались інтернетом щотижня, більшість дітей проводило принаймні три години на день, дивлячись телевізор, а час загалом витрачений на медіа дітьми дошкільного віку становив 47%. Також зазначається, що 36% дітей у віці від 2 до 11 років одночасно використовують обидва засоби. Загалом, діти у віці від 8 до 10 років щодня проводять близько 5,5 годин використовуючи носій [47]. Використання домашнього інтернету зростає з віком. Кожен з трьох дітей віком від трьох до п'яти років використовує інтернет вдома, у порівнянні з 54% 6- 11-річних та 72 % з 12-17-річних. Компанія, що пропонує онлайн послуги щодо захисту дітей від небажаного вмісту мережі «Guardchild» наводить на своїй сторінці результати багатьох досліджень наукових установ і соціальних 220 інституцій

США: 21% дітей дошкільного віку мають доступ до стільникових телефонів, 90% дітей у віці 8-16 років бачили онлайн порнографію, 70% дітей віком від 7 до 18 років виконуючи домашнє завдання натикалися на порнографію в мережі, 31% підлітків у віці 12-18 років завідомо неправильно вказали свій вік, щоб отримати доступ до сайтів з віковими обмеженнями, 95% батьків не знають/не розуміють онлайн сленгу чи скорочень, що використовують їх діти, кожен п'ятий з підлітків у віці отримував повідомлення з пропозиціями сексуального характеру, а 1 з 33 – були переслідуваними в мережі, 65% 8-14 річних були втягнені в кібербуллінг19, 69% підлітків регулярно отримуючи повідомлення від незнайомих людей не повідомляють про це батькам чи опікунам [93]. Відповідні актуальні статистичні дані щодо України виявилось знайти досить складно. Всеукраїнське соціологічне дослідження, проведене Інститутом соціології НАН України в 2009 р., виявило тривожні тенденції: понад 28% опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі; 17% без коливань діляться інформацією про себе і свою родину (адреса, професія, графік роботи батьків, наявність цінних речей у домі тощо); 22% дітей періодично потрапляють на сайти для дорослих; 28% дітей, побачивши в інтернеті рекламу алкоголю або куріння, хоча б один раз спробували їх купити, а 11% − спробували купувати наркотики; близько 14% опитуваних час від часу відправляють платні SMS за бонуси в онлайн-іграх і лише деякі звертають увагу на вартість послуги. Лише у 18% випадків дорослі перевіряють, які сайти відвідує дитина, тільки 11% батьків знають про такі онлайн-загрози, як "дорослий" контент, азартні ігри, онлайн-насилля, кіберзлочинність [38].

Комітет ООН з прав дитини у 2011 р. відзначив, що відвідування порнографічних сайтів становило 70% усього трафіку на території України, а 5 млн. українських користувачів на місяць цікавляться дитячою порнографією Департамент молоді Ради Європи у 2012 р. провів онлайн-опитування щодо досвіду молоді, пов'язаного з мовою ворожнечі в інтернеті. За його результатами 19 умисні образи, погрози, дифамації і повідомлення іншим даних, що компрометують за допомогою сучасних засобів комунікації, як

правило, протягом тривалого періоду часу. 221 69% не знають, де можна отримати допомогу жертві мови ворожнечі онлайн, 78% респондентів не отримували освіти щодо безпечної поведінки в інтернеті [264]. За даними міжнародної асоціації «INHOPE», видалення матеріалів сексуального зловживання над дітьми в інтернеті допомагає попередити їх подальше перетворення в жертву злочинних посягань. Профайл жертв розміщення матеріалів сексуального характеру у 2014 р. виглядав таким чином: юнацтво – 21% (у 81% випадках жертвами стають дівчата), підлітки – 72% (у 13% випадків жертвами стають хлопці діти), 7% (у 6% випадків – діти обох статей) [64].

Водночас, незалежно від країни чи частини світу діти і молодь вважають інтернет невід'ємною частиною свого життя, благом, навіть якщо воно дороге, недостовірне або доступне лише за допомогою спільних пристроїв (як наприклад у деяких країнах Африки). Всесвітнє опитування показує, що діти вважають його правом людини, необхідністю [600]. З урахуванням віку діти та молодь мають право на особливий захист і консультування при користуванні інтернетом. «Це означає, що: 1. право на вільне вираження своїх поглядів та участь у житті суспільства, на те, щоб бути почутими та вносити свій вклад у вирішення питань. Поглядам повинна приділятися належна увага з урахуванням вашого віку, ступеня зрілості та без дискримінації; 2. можливість очікувати на отримання інформації мовою, що відповідає віку, а також на навчання безпечному користуванню інтернетом, в тому числі щодо захисту вашого приватного життя, з боку вчителів, вихователів, батьків чи опікунів; 3. обов'язок знати, що контент, який створюєте в інтернеті, або контент про дитину, що створюється іншими інтернеткористувачами, може ставати доступним у будь-якому куточку світу і завдавати шкоду гідності, безпеці, приватному життю або іншим чином шкодити особі та її правам у цей час або на наступних етапах життя. На запит такий контент повинен бути вилучений або видалений протягом розумно короткого періоду часу; 4. можливість очікувати на отримання чіткої інформації про те, який онлайнконтент та

поведінка є незаконними (наприклад, домагання в інтернеті), а також мати можливість повідомити про потенційно незаконний контент. Така інформація має бути адаптована до віку та обставин, а також повинні надаватись поради та підтримка з належною повагою до конфіденційності та анонімності; 5. 222 повинен надаватися спеціальний захист від втручання у фізичне, психічне та моральне благополуччя, зокрема, захист від сексуальної експлуатації та насильства в інтернеті та від інших форм кіберзлочинності. Крім того, право на освіту, яка покликане захистити від подібних загроз» [397].

Таким чином, виникає суперечлива ситуація. З одного боку, права дитини на доступ до інформації, на вільний розвиток, персональні дані тощо, з іншого – необхідність забезпечити захист від кіберзагроз та інформаційну безпеку дитини, в цілому. Хто і якою мірою має за це нести відповідальність? Англійська дослідниця С. Лівінгстон [61], підкреслюючи, що один з трьох користувачів інтернету є дитиною, наголошує, що із зростанням технологій дитячі організації, представники приватного сектору, регулюючі органи мають опікуватись тим, що права дітей потребують такої ж реалізації онлайн, як і оффлайн. Права дитини, викладені в Конвенції ООН прав дитини, дослідниця застосовує до онлайн середовища. Серед загроз з якими дитина зіткнутись при використанні комунікаційних технологій можна виокремити такі: технологічні: загроза як для дітей, так і для дорослих користувачів; доступ до інформації з неприйнятним (часто незаконним) змістом, зокрема, порнографічні, такі, що пропагують наркотики, психотропні речовини й алкоголь, тероризм і екстремізм, ксенофобію, сектантство,національну, класову, соціальну нетерпимість, нерівність, асоціальну поведінку, насилля, агресію, суїцид, азартні ігри, інтернет-шахрайство [234], розголошення персональних даних та іншої конфіденційної інформації, як власної, так і членів сім'ї, друзів чи знайомих, контакт з незнайомцями, що може призвести наслідків як у віртуальному (кібербулінг, дитяча порнографія тощо), так і реальному житті (сексуальне використання, фізичні ушкодження, викрадення). Не слід залишати поза увагою те, що інформаційна безпека, це не лише кібербезпека і не

обмежується безпечним перебуванням у віртуальному просторі. Реалізація численних прав і свобод дитини в сучасному суспільстві залежить від гарантування дотримання її інформаційних прав. Зокрема, це стосується права на рівень життя, необхідний для їх розвитку, права дітей на вираження своїх поглядів, право на існування власного майна, на свободу думки, совісті і релігії, асоціацій і мирних зборів, доступ дитини до поширення інформації, освіту, користування рідною мовою і культурою, сповідування своєї релігії, відпочинок і дозвілля. Чи можливим є регулювання взаємодії між медіа і дітьми? Протягом другої половини століття телебачення суворо звинувачувалося в поширенні багатьох соціальних хвороб, тепер цей акцент перенесено на інтернет.

Сучасні медіа переважно знаходяться в комерційному використанні, а отже основним регулюючим фактором є фінансовий. Ресурси, які раніше були призначені виключно для дорослих, тепер часто є доступними дітям. Глобалізаційні процеси в першу чергу в мережевому просторі дозволяють уникати регулювання національним законодавством. Подібною є ситуація щодо телебачення і радіомовлення. Оскільки аудіовізуальні технології спрямовані на сумісність з новими медіа20, національні регулятори стикаються з практично нереальними для вирішення завданнями - класифікації, обмеження або планування всього того, що з'являється на екранах країни, а тим більш не мають можливості впливу на споживачів. Виходячи із специфіки дитячого віку, слід сказати, що у профілактичній роботі з даною групою велике значення мають, насамперед, заходи не правового характеру, а педагогічні, психологічні, медичні [74]. Дослідження свідчать, що з точки зору батьків, ті фактори, які ускладнюють державне регулювання нового медіа-оточення, тягнуть за собою аналогічні складності і для батьків [19]. Батькам було складно відстежувати і впливати на зміст того, що переглядали їхні діти вдома чи у своїх друзів в епоху телебачення. Тим більш, це завдання ускладнилось в епоху інтернету і портативних технологій («гаджетів»). Таким чином, визначення змісту контенту, що споживають діти, виходить за межі можливостей батьківського

контролю. Крім цього, як свідчать знову таки дослідження, значна кількість батьків не до кінця розуміють сенс комп'ютерних ігор та сторінок в інтернеті, якими користуються їхні діти. Інтерактивні електронні засоби масової комунікації, засновані, переважно, на технологіях Web 2.0. На сторінці Майкрософт розміщені правила безпечного користування інтернетом. «Оскільки дорослі самостійно вирішують, який рівень конфіденційності потрібно забезпечити дітям, цей список рекомендацій містить орієнтовні правила користування комп’ютером, зокрема: відстежуйте використання інтернету; попросіть дітей ніколи не надавати особисті відомості, як-от ім’я, місцезнаходження, зображення, паролі, номери телефонів тощо; використовуйте програмне забезпечення для батьківського контролю; дозволяйте дітям переписуватися та спілкуватися лише з тими людьми, яких ви знаєте; розмовляйте з дітьми про незручні або неприємні ситуації в інтернеті; розкажіть дітям, що не слід відповідати на неочікувані або небажані повідомлення електронної пошти; пам’ятайте про те, що практично нічого в інтернеті не є повністю приватним» [37]. Існує думка, оскільки «інтернет здебільшого є продуктом приватних компаній, то реалізація та порушення прав людини в інтернеті має трьохсторонній характер: людина-приватна компанія (провайдер інтернет-послуг чи інтернетдоступу тощо) -держава» [503]. Така позиція, на нашу думку не є однозначною, оскільки гарантування прав і свобод на національному рівні залишається обов’язком держави, тому числі створення належного правового і організаційного забезпечення для їх реалізації. Тоді як зі сторони юридичних і фізичних осіб очікуваною і бажаною поведінкою є дотримання існуючих правових норм, не порушення прав інших учасників правовідносин та виконання покладених на них обов’язків. Повертаючись до питання щодо інформаційної безпеки дітей та молоді, важливо відзначити необхідність формування належного рівня інформаційної культури, в тому числі опанування навичок критичного мислення, культури безпечної поведінки в інформаційному просторі. Важливим учасником цього процесу є держава, оскільки саме вона через уповноважені органи встановлює зміст навчальних

програм, форми навчання і забезпечує підготовку педагогічних кадрів. Водночас аналіз листів МОН та регіональних органів виконавчої влади у сфері освіти, зміст яких присвячений проблемам інформаційної безпеки: Листи 225 МОН України "Про захист дітей та молоді від негативних інформаційних впливів", «Про проведення дня безпечного інтернету», «Про проведення конкурсу «Онляндія в моїй школі» свідчить про їх популістський і декларативний характер. Основним завданням взаємодії батьків, соціальних інституцій і держави в процесі навчання і виховання підлітків з питань інформаційної безпеки повинно бути формування у них інформаційно-комунікаційних компетентностей щодо користування інтернетом.

Зокрема серед таких компетентностей слід виділити:

1. Грамотний і успішний пошук інформації: розпізнавання інформаційних потреб; формулювання питань, що відображають інформаційні потреби; знання про існування багатьох інформаційних джерел; пошук, вибір і оцінка інформаційного джерела; зберігання інформації.

2. Критична оцінка інформації: розуміння змісту інформаційного повідомлення; вибір і оцінювання інформації; прийняття рішення про те, що є фактом, а що точкою зору; вирізнення рекламних текстів.

3. Творення, перетворення і презентація інформаційного змісту: творення нового інформаційного змісту; перетворення знайденого в інтернеті або раніше самостійно створеного інформаційного змісту; презентація нового або перетвореного інформаційного змісту.

4. Правові засади творення й поширення інформаційного змісту: усвідомлення правового й етичного вимірів творення інформації; знання, який інформаційний зміст можна перетворювати відповідно до правових засад; знання своїх прав як творця інформації, розміщеної в інтернеті; усвідомлення різниці між інтернет-комунікацією й спілкуванням поза інтернетом.

5. Емпатія й образотворення: знання про те, що інтернет є простором спільної комунікації з іншими людьми; виявлення емпатії в мережі; створення обдуманого й адекватного власного образу.

6. Безпека і приватність: знання про загрози, пов’язані з перебуванням в інтернеті; уміння запобігти небезпекам в інтернеті; здійснення контролю над інформацією, яка передається іншим; усвідомлення різниці між інтернет-комунікацією й спілкуванням поза інтернетом; застосування гігієнічних засад, пов’язаних з використанням комп’ютера.

7. Участь у соціальних електронних мережах: розпізнання елементів інтернеткультури; активна участь у мережних соціальних спільнотах; ініціативність в розвитку мережних соціальних спільнот, створених для спільних дій [228].

Важливим є створення умов для співпраці батьків та осіб, що їх замінюють, з відповідними органами, що можуть надавати допомогу у випадку актуалізації загроз інформаційній безпеці дітей. Досвід такої допомоги є різний – від створення відповідних підрозділів поліції до сприяння громадським організаціям, які забезпечують роботу інфоліній у випадку виникнення загрози (наприклад, при кібербулінгу чи кібермоббінгу), відслідковують дитячу порнографію онлайн і повідомляють уповноважені органи, а також здійснюють просвітницьку роботу як серед дітей та молоді, так і для батьків та осіб, що ними опікуються. Процес комп’ютеризації шкіл, що відбувається сьогодні, безперечно, є прогресивним явищем, але без відповідної методичної підтримки, без перепідготовки учителів-предметників, без інтеграції комп’ютерних технологій у навчальний процес не буде забезпечено належного їх використання. Використання технологій мультимедіа при викладання всіх шкільних дисциплін дозволить підвищити якість засвоєння знань, а також зростання рівня індивідуалізації навчання, що є особливо важливим для дітей з особливими потребами. За оцінками Всесвітньої організації охорони здоров’я, понад 1 мільярд людей мають якусь форму інвалідності, а це майже 15% населення світу. В Україні понад 2 мільйони 800 тисяч людей мають статус інваліда, з них 151 тисяча – діти. Це 6,1 відсотка до загальної кількості населення. І майже 80 % інвалідів – це люди працездатного віку.

Особи з обмеженими фізичними можливостями, особливостями інтелектуального розвитку та психічними порушеннями часто бувають виключені з повноцінного життя, зіштовхуючись з дискримінація різних форм, включно з фізичними і соціальними бар’єрами. Поняття повноправного члена суспільства, яке є результатом соціалізації, має на увазі, перш за все, визнання членами суспільства іншого як рівного [142]. Інформаційні технології мають значний потенціал для покращення якості життя багатьох людей з обмеженими можливостями. Водночас, можуть стати бар'єром, для прикладу, якщо сторінка має занадто дрібний шрифт, інформація на ній недоступна людям з вадами зору; відсутність написів адаптованих для скрінрідерів - додатків, які озвучують текст на екрані – стає перешкодою для незрячих людей; якщо сторінка не містить транскрипти аудіофайлів – інформація недоступна для глухих і слабочуючих людей, це лише найочевидніші перешкоди. Окрім того, що в суспільстві існує стереотипне мислення і велика проблема під назвою ейблізм21 [68], то ще й категорія «нормальності» викликає поділ на тих, хто є «нормальним», і тих, хто «нормальним» не є, - поділ на «ми» і «вони» і, як наслідок, аутгруппову гомогенність [589]

Дослідниця Енн Гібсон змогла нарахувати як мінімум 26 різних ситуацій, коли можливості людей обмежені і у них виникає потреба в доступному інтернеті, наприклад, «хтось впав і зламав пальці - тепер для навігації в інтернеті він може використовувати тільки ліву руку і клавіатуру; хворому на епілепсію, яка іноді викликається яскравими контрастними кольорами, потрібно з обережністю відвідувати сайти з яскравим дизайном; військовослужбовець, що служив на плавучому маяку і, як це трапляється з багатьма, став погано чути на одне вухо - він повертає голову в бік звуку на комп'ютері, але так йому складно бачити екран; а у батьків малих дітей немає фізичних обмеженостей, проте якщо їх більш ніж один, наприклад близнюки, яким по одному року, і це вже успіх, якщо, коли тримаючи когось із них на одній руці, залишається хоча б один вільний палець на іншій руці для навігації по iPad або включення Siri»[589].

У 1999 р. Консорціум Всесвітньої павутини, що займається розробкою єдиних принципів і стандартів для інтернету, створив список рекомендацій WCAG 1.0 (Web Content Accessibility Guidelines), спрямований на забезпечення доступності ресурсів Всесвітньої павутини для людей з обмеженими фізичними можливостями, у 2008 р. вийшла його друга версія рекомендацій WCAG 2.0. У жовтні 2012 р. WCAG 2.0 була прийнята Міжнародною організацією стандартизації як Міжнародним стандартом ISO, ISO / IEC 40500: 2012 [643].

Від англ. Ableism — це системна дискримінація людей з хронічними захворюваннями та інвалідністю. Ейблізм характеризує людей, орієнтуючись тільки на їх порушення і ставить їх потреби на другий план, порівняно з іншими людьми. Саме через це, людям з інвалідністю приписують або навпаки відмовляють у певних навичках або рисах характеру. Ефект аутгрупової гомогенності проявляється в схильності бачити членів своєї групи як різноманітних індивідів, а члени чужій групи здаються нам схожими один на одного. В результаті ми уявляємо собі людей з обмеженими можливостями дуже типовим чином - сліпі з білою тростиною, глухі зі слуховими апаратами, люди на інвалідних візках.

Для осіб з обмеженими можливостями доступність - це можливість використовувати продукт або послугу так само ефективно, як це робила би здорова людина. Це означає, що потрібно використовувати принципи дизайну, які забезпечують доступність продуктів і послуг для більшої кількості людей. У деяких випадках це неможливо, тому для компенсації можуть використовуватися допоміжні технології. Якщо це так, поширені технології повинні забезпечувати безпроблемне програмне або апаратне підключення допоміжного пристрою, як в плані взаємодії, так і в плані портативності даних [127]. Знов таки, як і будь яка соціальна проблема, можливість реалізації прав і свобод людини з обмеженими можливостями в інформаційному суспільстві є комплексною, і її вирішення залежить від співпраці держави, громадянського суспільства, бізнес структур, міжнародного співтовариства і самої особи з обмеженими можливостями. При цьому кожному з них відведено власна роль.

Для прикладу, бізнес-група по доступним ІКТ розробила Хартію за доступними технологіями в листопаді 2011 р.. Хартія містить 10 зобов'язань, які повинні дотримуватися корпорації, щоб доступність ІКТ була реалізована у всій організації, включаючи відділ кадрів, політики, поінформованість персоналу, зміни на робочих місцях і закупівлі. Першими цю хартію підписали 17 провідних компаній, включаючи Cisco, Fujitsu, Microsoft і Oracle [126].

Держави ж зобов’язані створити таке правове поле, в якому були б гарантовані права і можливості осіб з обмеженими можливостями. Як свідчить міжнародний досвід, це можливо реалізувати різними шляхами. Наступна категорія - люди, що здійснюють діяльність, яка має або може мати важливі соціальні наслідки - є надзвичайно широкою і неоднорідною. Об’єднати державних службовців, медійних осіб та журналістів, правозахисників, громадських активістів і політичних діячів в одну групу з метою дослідження особливостей загроз їх інформаційній безпеці спонукало суспільна значимість їх діяльності. Адже кожен із них є публічною особою, має власну аудиторію, на яку чинить інформаційний вплив, а окрім того виконує важливу державну чи/та суспільну функцію.

На поверхні знаходяться конфлікти між правом публічних осіб на приватність та правом на свободу вираження поглядів, правом на захист персональних даних і правом доступу до публічної інформації тощо. Ця тема неодноразово досліджувалась в наукових працях, як вітчизняних, так і зарубіжних, існує низка судових прецедентів в національних судах та Європейському Суді з прав людини. Питання балансу між правом на свободу вираження поглядів і захистом права на приватне життя є досить неоднозначним. [547]. Нагнічук О. І. на підставі аналізу практики Європейському Суді з прав людини формулює принципи співвідношення права на свободу вираження та права на приватність щодо публічних осіб:

1) будь-яке втручання в приватне життя можливе настільки, наскільки це сприяє публічним дебатам з питань загальної важливості;

2) якщо зображення особи, яка вийшла на публічну арену, не містить інформації про її приватне життя, воно може використовуватися, незважаючи на те, чи є ця особа відомою;

3) особи, які стали публічними не з власного бажання, користуються більшим захистом приватного життя порівняно з іншими публічними особами;

4) публічні особи мають право бути захищеними від поширення пліток про їхнє приватне життя;

5) почуттям родичів і близьких померлої публічної особи може бути спричинено шкоду розголошенням конфіденційної інформації про публічну особу, але чим більше часу проходить після смерті публічної особи, тим більше суспільний інтерес в отриманні такої інформації перевищує необхідність конфіденційності такої інформації;

6) не може бути конфіденційною інформацією ставлення політиків до суспільних явищ;

7) комерційні питання не є сферою приватного життя публічної особи [265].

Водночас, право на доступ до інформації, якою володіють органи публічної влади, є основоположним правом людини, а також гарантією функціонування демократичної держави. Право на доступ до інформації вимагає від держави не 23 Проаналізовані були справи Cumpana and Mazare v. Romania (App no 33348/96) ECHR 17 December 2004, Tammer v. Estonia (App no 41205/98) ECHR 06 February 2001; Karhuvaara and Italenti v. Finland (App no 53678/00) ECHR 16 November 2004; Standard Verlags Gmbh. v. Austria (2) (App no 21277/05) ECHR 04 June 2009. 12; Thorgeir Thorgeirson v. Iceland (App no 13778/88) ECHR 25 June 1992; Edition Plon v. France (App no 58148/00) ECHR 18 May 2004; Craxy (2) v. Italy (App no 45737/16) ECHR 17 July 2003; Fressoz and Roire v. France (App no 29183/95) ECHR 21 January 1999; Társaság a Szabadságjogokért v. Hungary (App no 37374/05) ECHR 14 April 2009. утримання від втручання, а активних дій – забезпечення нормативних, організаційних та технічних умов реалізації права на інформацію, у тому числі належного

розгляду запитів на інформацію та оприлюднення в ініціативному порядку суспільно важливої інформації. Однак порушення балансу між цими правами призводить до виникнення загрози основним демократичним цінностям, адже право на доступ до інформації є правом інструментальним, тобто таким, що необхідне для реалізації інших прав і свобод людини, – без доступу до певної інформації, яка знаходиться в органів влади чи інших суб'єктів, людина часто не може реалізувати свої інші права (наприклад, на доступ до суду, участь у виборах та в управлінні державними справами, на освіту тощо). Окрім того, діяльність осіб, яка має соціальне значення, створює значну кількість обставин, що стають передумовами для втручання в приватне спілкування, що здійснюється як санкціоновано – державними уповноваженими органами (право ініціювати таку діяльність мають Національна поліція, Державне бюро розслідувань, Служба безпеки України, Служба зовнішньої розвідки, Державна прикордонна служба, Управління державної охорони, Фіскальна служба, Національне антикорупційне бюро), так і неправомірно – журналістами, політичними опонентами та бізнес-конкурентами. Згідно ст. 9 Закону України «Про телекомунікації» «охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом» [155]. При цьому на операторів, провайдерів телекомунікацій покладено зобов'язання вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами (ч.3 ст.9).

Кримінально-процесуальним кодексом України передбачено, що для втручання у приватне спілкування необхідна ухвала слідчого судді. При цьому під спілкуванням розуміється передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв’язку будь-якого

типу. Спілкування вважається приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб.

Стаття 258 КПК України визначає різновиди втручання в приватне спілкування є:

1) аудіо-, відеоконтроль особи;

2) арешт, огляд і виїмка кореспонденції;

3) зняття інформації з транспортних телекомунікаційних мереж;

4) зняття інформації з електронних інформаційних систем [219].

Але навіть, за умови дотримання процедури втручання слід пам'ятати, що зняття такої інформації часто зачіпає права і законні інтереси третіх осіб. Важливими гарантіями захисту прав людини при здійсненні втручання в приватне спілкування є: дотримання принципу законності – як щодо процедури, так і щодо обґрунтованості винесенні суддею відповідної ухвали, надійне і обмежене в часі матеріалів, а також невикористання і негайне знищення матеріалів,що не стосуються справи і порушують права третіх осіб. Прослуховування, фотографування чи відео зйомка є доступними і часто використовуються в незаконних цілях. Поширеним прикладом останнім часом стало фотографування в парламенті та поширення особистої переписки народних депутатів, переважна більшість таких даних не пов'язана з державницькою діяльністю депутатів, є їхньою конфіденційною інформацією. Більше того, поширення фотознімків такої переписки також часто шкодить третім особам, які спілкуються з депутатами, проте не перебувають на державних посадах (наприклад, журналістам, знайомим публічної особи) [319]. Не до кінця врегульованою з точки зору захисту прав третіх осіб залишається ситуація з оприлюдненням електронних декларацій. Безперечно, схема електронного декларування в Україні є важливим кроком у боротьбі з корупцією. Головними завданнями е-декларування є контроль і протидія незаконному збагаченню. Іншим аспектом е-декларування, на думку В. Чумака,

є політичний, а 232 конкретніше той факт, що ці декларації депутатів можуть стати додатковою інформацією для виборців [109]. При цьому не слід забувати, що поруч з інформацією про осіб, уповноважених на виконання функцій держави або місцевого самоврядування, при поданні е-декларацій розкривається інформація їх членів сім'ї. Водночас, самі декларанти висловлювали побоювання, що «відкрите електронне декларування майна чиновників "дає пряму наводку для злочинців" та є питанням безпеки сотень тисяч людей» [528], а також що воно стало «інструментом тиску на суддів для того, аби схиляти їх до прийняття тих чи інших рішень» [111].

При користуванні соціальними мережами необхідно враховувати параметри їх конфіденційності з метою відповідального їх використання, моніторингу та регулярного аналізу власних соціальних мереж та контентів, що розміщуються в соціальних мережах. При виявленні в них помилок або будь-яких невідповідностей конфіденційності вони підлягають негайному виправленню та/або видаленню. У соціальних мережах адвокатам рекомендовано обережно відноситись до коментарів, які можуть відображати позицію, що протилежна позиції клієнта. При встановленні адвокатом контактів та спілкування у соціальних мережах, інтернетфорумах та інших формах спілкування в мережі з клієнтами, колегами, суддями, процесуальними опонентами та іншими особами та їх об'єднаннями, він зобов'язаний виключити можливість виникнення конфлікту інтересів. Висловлювання адвоката в соціальних мережах, інтернет-форумах та інших формах спілкування в мережі не повинні мати притаманний правовий нігілізм, будь-який вид агресії, ворожнечі і нетерпимості. Адвокат зобов'язаний вести себе шанобливо і не допускати образливої поведінки. Будь-які заяви, коментарі адвоката в соціальних мережах, інтернет-форумах та інших формах спілкування в мережі інтернет, в тому числі під час обговорення і роз'яснення правових норм, особливостей судочинства, дій його учасників, повинні бути відповідальними, достовірними і не вводити в оману [328].

Така сувора регламентація, водночас, залишає відкритим питання ідентифікації особи у соціальних мережах. Адже одна із головних цінностей інтернету – це можливість зберігати анонімність. Наприклад, адвокат О. Шевчук із цього приводу зазначив, що в соціальних мережах неодноразово відкрито принижується честь і гідність не лише окремих адвокатів, а й діяльності української адвокатури загалом [327]. При цьому допускається варіант заохочення до поширення технічних знань і можливостей в економіці; сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках; побудову та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудову глобальних систем комунікації і дослідження впливу систем на міжнародні, національні та приватні пріоритети; збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційність інформації, інформацію як суспільне благо, інформацію як товар, інформацію як невіддільний компонент існування держави; недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях і в різних сферах державного управління та в приватному секторі; творення урядової політики в галузі інформації і комунікації [436,с.24-25].

2.4. Підходи до державного регулювання відносин у сфері інформаційної безпеки в зарубіжних країнах

Політика Європейського Союзу, що мала на меті зміцнення стосунків зі східними сусідами ЄС і продовженням східного напрямку існуючої Європейської політики сусідства під назвою «Східне партнерство» була відкрита Європейським Союзом у 2009 р. Вона стосується шести країн пострадянського простору - України, Білорусі, Молдови, Вірменії, Грузії та Азербайджану. Хоча останнім часом точиться значна кількість дискусій щодо перспектив, так, глава МЗС Польщі В. Ващиковський, коментуючи

перспективи «Східного партнерства» заявив, що «програма відводила згаданим державам лише роль буферної зони між 312 Росією та ЄС» [533].

Проте, власне ці два фактори – (1) проевропейська політична спрямованість, а отже і спроби адаптації до законодавства і стандартів ЄС, а також (2) геополітична ситуація, що обумовлена значним впливом Російської Федерації, і визначили вибір цих країн задля дослідження соціально-правових питань інформаційної безпеки людини. На сьогодні простежується тенденції певної диференціації в рамках "Східного партнерства", коли три країни - Україна, Грузія і Молдова – більш інтенсивно рухаються в напрямку ЄС, оскільки всі вони підписали Угоду про асоціацію з ЄС, а також отримали безвізовий режим. У Молдові розроблений значний масив законодавчих актів в інформаційній сфері, до яких належать: Конституція, (ст. 32 Свобода думок і вираження; ст. 34 - Право на інформацію); Закон про свободу вираження поглядів (2010); Закон про пресу (1994); Закон про доступ до інформації (2000); Закон про прозорість процесу прийняття рішень (2008); Закон про захист персональних даних (2007, та нова редакція 2011); Закон про народного адвоката - омбудсмена (2014 р.); Закон про електронні комунікації (2007); Кодекс телебачення і радіо Республіки Молдова (2006); Закон про запобігання та боротьбу з кіберзлочинністю (2010). Поруч із певними позитивними напрацюваннями мають місце загрозливі тенденції, втому числі пов’язані з проблемами реалізації положень законодавства. Зокрема, на думку експертів, мають місце випадки, коли положення Закону «Про захист персональних даних», а також Закону «Про державну таємницю» використовується владою, щоб обмежити публічний доступ до інформації.

Починаючи з 2010 р. в Молдові розробляється електронне урядування. У 2010 р. створений Урядом Республіки Молдова Центр електронного урядування (www.egov.md), діяльність якого спрямована на забезпечення громадян країни публічною інформацією та послугами в режимі «нон-стоп», а також прозорості діяльності органів державного управління шляхом використання та просування інформаційних технологій в публічному секторі. За цей час реалізовано низку

ініціатив для громадян, бізнесу, уряду, зокрема, введено в дію спрямовані на громадян сервіси: «Платформа відкритих даних», «Єдина платформа для публічних послуг», «Мобільний підпис», «Е-довідка про несудимість», «Реєстр 313 місцевих актів». Зокрема, завдяки Платформі відкритих даних (www.date.gov.md.) уряд забезпечує доступ громадян та підприємств і організацій до пакетів даних публічного характеру, а єдина платформа публічних послуг (https://servicii.gov.md/) фактично є каталогом публічних послуг органів державної влади. Розроблена і впроваджена послуга «мобільний підпис», що дозволяє за допомогою мобільного телефону отримувати дозволяючи при цьому ідентифікувати та підтверджувати особу у віртуальному просторі. За допомогою послуги «мобільний підпис» громадяни мають доступ до електронних послуг - засвідчення документів, електронна звітність, декларування тощо

Портал «Реєстр місцевих актів» (www.actelocale.md) дозволяє громадянам та бізнесу мати доступ до централізованої бази актів органів публічної влади Молдови. Цінними для бізнесу є послуги «Е-ліцензування», «Швидка декларація», «Електронна декларація». Для органів державної влади введено сервіси: «Реєстр персональних даних», «Particip.gov.md», «M-pass». Упровадження платформи «Particip.gov.md» достосовано до потреб партисипативної демократії, яка проваджується в Молдові з метою подолання недоліків представницької демократії. Використовується платформа у консультаціях з громадянами щодо проектів нормативних актів, для розсилки новин, а також генерування спеціального коду, що спрощує процедуру інформування про появу проектів актів, що становлять публічний інтерес. Ця платформа позиціонується як елемент Програми «Національна стратегія розвитку «Молдова 2020». Послуга «M-pass» через мобільний підпис, цифровий сертифікат або пароль забезпечує ідентифікацію осіб, що звертаються за електронними послугами. Проте системи е-демократії є вразливими з точки зору інформаційної безпеки. Хакери атакували урядову автоматизовану інформаційну систему «Вибори» під час референдуму 2010 р..

Референдум стосувався змін Конституції, і проведені атаки призвели до дублювання даних в системі. Хакери, як з'ясувалося, домагалися, щоб референдум був визнаний недійсним, але результати їх дій виявилися незначними і лише відклали оголошення підсумків референдуму, а не скасували їх [273]. У Молдові вчиняється значна кількість кіберзлочинів, в основному це: порушення таємниці листування, порушення авторських прав, розголошення таємниці, поширення дитячої порнографії і несанкціонований доступ до мереж і телекомунікаційних послуг. Окрім того, правоохоронні органи розслідують все більше кіберзлочинів, пов'язаних з порушенням недоторканності приватного життя. Відділ інформаційних технологій та розслідувань кіберзлочинів Генеральної прокуратури зайнятий питаннями, пов'язаними з фальсифікацією особистих облікових записів в соціальних мережах, незаконним видаленням особистого листування з електронної пошти і SMS, а також захопленням офіційних облікових записів з метою відправки фішинг-повідомлень. з метою охорони права інтелектуальної власності було розпочато розслідування файлообмінного сайту Torrentsmd.com. Нестійка економіка Молдови створює сприятливі умови для фінансових кіберзлочинів.

Часто, фінансові злочини вчиняються у змові з громадянами інших країн СНД. Наприклад, група з 37 осіб переважно з Росії та Молдови була притягнута до відповідальності за ретельно опрацьовану схему по відмиванню грошей та хакінгу. Фізичні особи в Молдові і Росії зламували комп'ютери дрібного і середнього бізнесу і заражали їх троянської програмою Zeus, яка поставляла паролі іноземцям, котрі перебувають в США на підставі студентських віз, які по ним знімали гроші і відправляли їх своїм ватажкам. Так кіберзлочинці здійснили крадіжку понад 70 мільйонів доларів [273].

Злочинність зі звичного середовища має своє продовження в інтернет. Молдова, що відноситься до країн 2-го рівня відповідно до звіту Держдепартаменту США по боротьбі з торгівлею людьми, має проблему щодо ліквідації торгівлі людьми. Нові технології означають, що «традиційні» злочини переходять в онлайн-простір; викрадачі використовують смартфони,

комп'ютери та інтернет, щоб вимагати гроші і перевозити жертв через кордони. Зокрема, спостерігається значний підйом використання інтернету для рекрутингу та експлуатації жертв. У Молдові був створений спеціальний відділ по боротьбі зі злочинністю, що спеціалізується на злочинах сексуального характеру проти дітей [273].

Молдова, як і раніше залишається притулком для піратства і порушень авторських прав - надзвичайно високий рівень поширення піратського програмного забезпечення; за приблизною оцінкою 90 % всього програмного забезпечення в країні поширюється незаконно. Ситуацію погіршує той факт, що більшість таких справ закриваються без суду і винесення вироку. Мають місце і порушення інформаційних прав громадян. Молдова має багатоцільову централізовану базу даних по всіх громадянах під назвою «Registru». У «Registru» агрегована інформація, зібрана державними органами. Урядові установи і організації можуть отримати доступ до бази даних на підставі спеціальної угоди, в якому вказані їх допуски і обмеження. Організації з захисту прав людини постійно звертають увагу на занадто розширене призначення цієї бази даних, і те, що їй не вистачає контролю, що може привести до безпрецедентного рівня державного нагляду. Незважаючи на стурбованість щодо приватної інформації «Registru» надалі функціонує. Онлайн-нагляд в Молдові не так розвинений, як в інших країнах СНД, проте правове поле розвивається повільно. У грудні 2012 р. увійшов в силу новий Закон про спеціальну розшукову діяльність з поправками щодо законного перехоплення повідомлень, а також змін обов'язків і функціоналу відповідних інстанцій. Винятковим правом законного перехоплення повідомлень як і раніше володіє Національна служба інформації і безпеки, яка в цих цілях співпрацює з провайдерами мережевих послуг і послуг електронного зв'язку. Крім того, в 2012 р. прийнято поправки до кримінально-процесуального кодексу, які ввели процедуру законного перехоплення електронного зв'язку і даних, зібраних провайдерами послуг. Закон накладає ряд обов'язків на власників комп'ютерних систем, доступ до яких заборонений або обмежений для деяких категорій

користувачів. Вони зобов'язані попередити користувачів про правові умови доступу та користування, а також про юридичні наслідки несанкціонованого доступу до цих комп'ютерних систем. Попередження повинне бути доступно для кожного користувача. У той же час ряд зобов'язань накладається на постачальників послуг. Вони ведуть облік користувачів і повідомляють компетентним органам дані про інформаційні потоки, в тому числі про нелегальний доступ до інформації з 316 комп'ютерних систем, спробах впровадження незаконних програм. Провайдери зобов'язані повідомляти про порушення відповідальними особами правил збору, обробки, зберігання, поширення і розподілу інформації або правил захисту комп'ютерної системи, якщо ці дії спричинили серйозні наслідки, наприклад, сприяли присвоєнню, перетворенню або знищення інформації, порушили роботу комп'ютерних систем. У зв’язку з тенденціями інформаційних впливів, зараз у Молдові розглядаються відразу кілька законодавчих ініціатив, пов'язаних з регулюванням блокування інтернет-ресурсів, повноважень правоохоронних органів і покладених на провайдерів зобов'язань. У 2016 р. була розроблена нова концепція інформаційної безпеки [615]. У драфті проекту два ключових елементи: (1) кібер-безпека - захист критичної інфраструктури, захист від кібер-атак, збереження цілісності даних тощо, (2) інформаційна безпека - все що стосується інформаційних воєн, пропаганди і дезінформації. Прийняття цієї концепції може стати важливим кроком, проте в проекті спостерігається проблема, типова також і для України, - кібербезпека ототожнюється з інформаційною безпекою, відсутній визначений понятійний апарат, а також стратегічний підхід до вирішення проблеми. Гарантом громадських інтересів в сфері телебачення і радіомовлення покликана бути Аудіовізуальна Координаційна Рада. Рада задекларована як незалежний інститут, але часто ця "незалежність" викликає сумніви. Вона наділена недостатньою кількістю інструментів для того, щоб ефективно регулювати медійний ринок і карати порушників. Найчастіше мають місце публічне попередження, штраф, призупинення права на трансляцію реклами на певний період, про

призупинення ліцензії на мовлення протягом певного періоду або (вкрай рідко і зазвичай політично мотивовано) анулювання ліцензії. Після зміни влади в 2009 р. на "про-європейську" значно покращилась ситуація з цензурою. Раніше державні ресурси використовувалися з метою тиску на вільні ЗМІ і політичних опонентів. Проте, на сьогодні, має місце монополізація інформаційного ринку, зокрема ЗМІ. А вже згадана Аудіовізуальна координаційна Рада не має достатніх важелів впливати ні на внутрішній інформаційні війни (між 317 політичними гравцями), ні на зовнішні інформаційні впливи (як з боку Росії, так і зі сторони Румунії). У 2014 Рада заборонила ретрансляцію Росія-24, але цим справа і обмежилося. Триває розробка проекту нового Кодексу телебачення і радіо Республіки Молдова, який, ймовірно, міститиме норми про заборону російських інформаційних каналів. Хоча щодо цього питання триває політичне протистояння, оскільки у авторів, окрім завзяття боротися з пропагандою, є також і власні фінансові та політичні інтереси. Також з 2013 р. правоохоронні органи все пробують «проштовхнути» низку законопроектів для боротьби з дитячою порнографією. Для цього хочуть змінити ряд законів: Кримінальний кодекс, Закон про електронні комунікації, Закон про попередження та боротьбу зі злочинністю сфері комп'ютерної інформації і т.д. Поки що це лише ініціативи, які не підтримав парламент. Грузія вирізняється серед інших колишніх радянських республік як найбільш прозахідна, за винятком країн Прибалтики. Нормативно-правове регулювання країни, в тому числі в сфері інформаційній сфері, змінювалося, з метою наближення до вимог членства Світової організації торгівлі та участі в програмі Східного партнерства Європейського союзу (ЄС), а в перспективі також і вимогам вступу в ЄС і НАТО. Організація «Freedom House» окреслила ситуацію в сфері засобів масової інформації як найбільш ліберальну і плюралістичну в регіоні в 2013 р., проте наголошується зростаюче занепокоєння з приводу політичного впливу на основні канали мовлення. Медійне середовище відрізняється різноманітністю, але при цьому поляризованим характером. Наслідки російсько-грузинської війни 2008 р., в ході якої відбулася одна з перших кібератак в умовах

міждержавного конфлікту, показали вразливість Тбілісі в інформаційному та кіберпросторі. Як наслідок, уряд Грузії посилив інформаційну політику, в тому числі підтримку вільного інтернету і запобігання цензурі.

В цілому можна говорити про ліберальність телекомунікаційної галузі. Інформаційно-комунікаційні технології щораз більше інтегруються в економіку, суспільне життя і політику країни. Відомості про контроль і нагляд нечисленні, 318 урядові заходи блокування онлайн-контенту відсутні. При цьому все-таки спостерігається деякий брак прозорості телекомунікаційної сфери. Склад власників медіакампаній зачасту приховується за фіктивними фірмами і компаніями в офшорних зонах. Конституція Грузії визначає, що «особисте життя кожної людини, його робоче місце, особисті записи, листування, переговори по телефону або з використанням інших технічних засобів, а також отримані за допомогою технічних засобів повідомлення недоторканні» (ст.20). Також, стаття 24 Конституції захищає право кожного громадянина «вільно отримувати та поширювати інформацію, висловлювати і поширювати свої думки в усній, письмовій чи іншій формі. Засоби масової інформації є вільними. Цензура забороняється». Конституційні засади втілені в нормах галузевого законодавства, зокрема, Законами «Про електронні комунікації», «Про інтелектуальну власність», «Про інформаційну безпеку», «Про мовлення» та інші. Закон «Про електронні комунікації» встановлює принципи розвитку конкурентного середовища в сфері комунікацій, регламентує права і обов'язки учасників правовідносин, визначає засади передачі персональних даних, а також визначає сферу компетенції національного органу регулювання зв'язку - Національної комісії Грузії з комунікацій. Національна комісія наділена двома основними механізмами забезпечення дотримання встановлених норм: відкликання ліцензій на роботу і накладення штрафів за недотримання, до 3 % доходу оператора після третього порушення. Штрафи та відкликання ліцензій не вимагають санкціонування судом, але в суд можна подати апеляцію, і протягом цього часу санкції будуть

продовжувати діяти. Серед соціальних мереж за кількістю користувачів в Грузії лідирує Facebook.

Хоча в інтернет-просторі Грузії широко використовується російська мова. Російськомовна блогосфера в Грузії більше політизована, ніж англо- або грузиномовний інформаційний простір. Певною мірою це обумовлено бажанням спілкування блогерів з колегами на пострадянському (а отже російськомовному) просторі. 319 Інтернет посідає друге за важливістю місце серед джерел новин та інформації після телебачення. Результати опитування показали, що 6 % респондентів дізнаються новини політики онлайн, а ще 12 % вважають інтернет в цілому важливим джерелом інформації [272].

Для онлайн-джерел новин не встановлено вимоги ліцензування, вихід на цей ринок відрізняється мінімальними перешкодами і низькою собівартістю. Онлайн-журналістика в Грузії характеризується високою якістю і виграє від здорового рівня плюралізму. На відміну від телевізійних станцій онлайн-ресурси меншою мірою залежать від політичного тиску. Доступ до всіх можливостей електронного врядування відкритий на одному сайті: http://e-government.gov.ge, серед доступних послуг, наприклад, можливості: перевірити виписані на громадянина штрафи на сайті поліції; замовити закордонний паспорт на сайті громадянського реєстру он-лайн, так само - отримати будь-яку довідку; поспілкуватися з відеоконсультантом на сайті міністерства фінансів і з'ясувати, які податки потрібно сплатити у тому чи іншому випадку, в тому числі, прямо на сайті розрахувати вартість розмитнення авто; підготуватися до здачі тестів на водійські права; перевірити дійсність будьякого завіреного нотаріусом документа у банку нотаріальних даних та інші [131].

Для Грузії, як і для України, суттєве значення має інтеграція з ЄС. Отримання безвізового режиму та підписання асоціації продемонстрували грузинським громадянам відчутну вигоду від проведених в країні реформ. Хоча демократичний розвиток Грузії переживає значні труднощі, як з огляду на складну геополітичну ситуацію, так і враховуючи слабкі опозиційні сили всередині держави [588]. Це ще одна причина, яка робить цінним вивчення

досвіду Грузії у сфері безпеки, зокрема, інформаційної. Білорусь. Інформаційна політика Республіці Білорусь є досить суперечливою. Республіка входить в число «Країн під наглядом», відповідно до рейтингу «Репортерів без кордонів», і раніше навіть вважалась «Ворогом інтернету». Але з технічної точки зору приватне використання інтернету здійснюється без значних обмежень. Швидкість з'єднання, легкість доступу і тарифи досить конкурентоспроможні, навіть в порівнянні з розвиненими країнами.

Конституція Білорусі [205] закріплює такі прав в інформаційній сфері: ст. 28 (право на недоторканність приватного життя); ст. 33 (право на свободу думок); ст. 34 (право на загальнодоступну інформацію). Положення Конституції заклали основу для регулювання інформаційної сфери: Закон «Про інформацію, інформатизацію і захист інформації» (2008) [281] містить положення щодо права на інформацію; загальнодоступної інформації та її класифікація; інформації, поширення і (або) надання якої обмежено, та її класифікація; права на захист інформації про приватне життя фізичної особи та персональних даних; службової інформації, а також регулює контент щодо широкого спектру питань, від безпеки даних до політики управління. Існує ряд спеціальних законів, які конкретизують права, закріплені в Конституції і Законі «Про інформацію»: «Про архівну справу та діловодство» [285] визначає право на доступ до архівних документів; «Про засоби масової інформації» - право на інформацію і свободу думок[1]; «Про електронний документ і електронний цифровий підпис», « Про авторське право і суміжні права» [284].

Регулювання інформації, поширення і (або) надання якої обмежено, здійснюється Законами: «Про державні секрети»[280]; «Про комерційну таємницю»; «Про охорону здоров'я» (норми, що визначають лікарську таємницю); Банківський кодекс (банківська таємниця) [23] та ін. З 2010 р. Білорусь активно розробляє національну політику в сфері ІКТ, на що частково впливає зростання соціальних мереж і їх вплив на білоруське суспільство. Регулювання інтернету переважно здійснюється на рівні президентських указів. Головним виконавчим органом в секторі телекомунікації є Міністерство зв'язку

та інформатизації і йому підпорядковано тринадцять організацій. Структурним підрозділом Міністерства є Республіканське унітарне підприємство з нагляду за електрозв'язком "БелГИЭ", і наділене широкими повноваженнями щодо інтернету, а саме контролює сектор електронних комунікацій, здебільшого щодо технічних стандартів, таких, як радіочастоти, накладає санкції на операторів або ініціює відкликання ліцензії провайдерапорушника; здійснює управління Центром реєстрації цифрових сертифікатів, надає послуги організаціям і приватним особам, а також адмініструє «чорний список» сайтів з обмеженим доступом в державних організаціях. Оперативно-аналітичний центр при адміністрації президента Республіки Білорусь, спочатку був підрозділом спецслужб (КДБ), а з 2010 функціонує як спеціалізований орган, безпосередньо підпорядкований президенту. Він контролює роботу провайдерів інтернет-послуг і управляє головним доменом республіки Білорусь (.by). Повноваження і обов'язки центру були розширені в 2011 р. і тепер включають криптографію, випущені державою електронні підписи і взаємодію між IT-системами державних інститутів. Вже згаданий Указ № 60 також вимагає, щоб провайдери інтернет-послуг блокували доступ до певної інформації в державних організаціях або за запитом конкретних користувачів. У секторі онлайн-новин домінують два політично нейтральних і незалежних ресурси: TUT.BY і Onliner.by.

У топ-50 найбільш часто відвідуваних веб-сайтів Білорусі є лише один абсолютно опозиційний ресурс - Charter97.org, який забезпечується командою з Польщі і Литви. Традиційні ЗМІ повністю контролюються державою. В країні немає незалежних місцевих новинних видань, а друковані ЗМІ залежать від економічних санкцій, які можуть негативно вплинути на тираж. Онлайн-платформи представляють собою єдиний відносно відкритий простір для вираження опозиційних або незалежних ідей, але вони можуть піддавати ризику тих, хто використовує їх для політичної пропаганди. У Білорусі немає спеціальних законів щодо кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і нормативними актами, що регулюють інтернет.

Відповідно до офіційної статистики, понад 90% кіберзлочинності в Білорусі мають фінансовий характер, а також мають місце: несанкціонований доступ до даних; диверсійні акти; незаконне отримання електронних даних; порушення правил використання комп'ютерних систем; а також створення, використання або розповсюдження шкідливого програмного забезпечення або комп'ютерних пристроїв

Інститут персональних даних також переживає етап становлення: відсутній відповідний закон, немає уповноваженого органу, а регулювання відбувається фрагментарно. Республіка Білорусь не приєдналася до Конвенції Ради Європи, яка визначає міжнародні стандарти в сфері захисту персональних даних. Основу політики щодо персональних даних складають закони «Про інформації, інформатизації та захисту інформації», «Про реєстр населення», «Про перепис населення». Відсутнє у республіці і законодавче визначення особливо чутливих/вразливих видів інформації, адекватного захисту їм не надається. Навіть в коментарях до закону про реєстр населення, які запропоновані Національним центром законотворчої діяльності термін «чутливі/вразливі дані» не вживається. «У реєстрі не буде ніяких даних, які можуть бути використані для будь-якого тиску на людину: про расу, національність і колір шкіри; про світогляд, політичних або релігійних переконаннях; щодо будь-яких захворювань; щодо сексуальної орієнтації; про усиновлення і багато інших»[19]. При цьому, у Білорусі нагляд за населенням здійснюється на національному рівні. Влада здійснює активний моніторинг протестів за допомогою обладнання для моніторингу російського виробництва, що використовується телекомунікаційними компаніями. Законодавство Вірменії в інформаційній сфері останні роки спрямоване на свободу, безпеку, а також економічного ефекту для всіх сфер (держави, суспільства, бізнесу та особистості). Нормативно-правова база у Вірменії розвивається з у рахуванням стандартів та норм ЄС. Телекомунікаційний сектор Вірменії одночасно ліберальний і відкритий бізнесу. Хоча спостерігається залишкова тенденція до надмірного регулювання кіберпростору. Норми інформаційного права містять

Конституція Республіки Арменії (зокрема, ст. 33. Свобода і таємниця обміну повідомленнями, ст. 34. Захист персональних даних, ст. 41. Свобода думки, совісти і релігії, ст. 42. Свобода вираження поглядів, ст. 51. Право на отримання інформації, ст. 53. Право на 323 подачу петицій), Кримінальний кодекс (містить норми щодо відповідальності за злочини проти безпеки комп'ютерної інформації), Цивільний Кодекс, а також закони Республіки Вірменії «Про свободу інформації», «Про електронну комунікацію», «Про державне сприяння сфері інформаційних технологій», «Про захист персональних даних» та інші. Дуже розвиненим, в тому числі на рівні міжнародних домовленостей, є законодавче регулювання у сфері інтелектуальної власності, зокрема, Закони «Про авторське право і суміжні права», «Про правову охорону топологій інтегральних мікросхем» та інші. Інформаційній безпеці на законодавчому рівні окремого акта не присвячено, в 2009 р. Радою національної безпеки було схвалено Концепцію інформаційної безпеки. Окремі положення містяться в Стратегії національної безпеки, Стратегії оборони та інших актах. Повноваження щодо забезпечення інформаційної безпеки також має низка органів, зокрема органи національної безпеки, міністерства оборони, поліція. Особливістю вірменської системи інформаційної безпеки є спрямованість на вирішення інформаційних проблем не тільки Вірменії, але і всього вірменства [282].

При цьому, як першочергові завдання цієї сфери виділяють:

1) інвентаризація наявних і формування нових інформаційних ресурсів, розробка системи їх ефективного співробітництва і безпечної діяльності;

2) концептуальна розробка методів внутрішньої і зовнішньої пропаганди/контрпропаганди і їх практична реалізація;

3) створення взаємодоповнюючих брендів вірменства і Вірменії, впровадження цих брендів - як елементи свідомості - у вірменському середовищі і в інших спільнотах;

4) розробка і реалізація суспільно-політичних, наукових, навчальних та інших загальнонаціональних проектів;

5) широке застосування сучасних технологій інформаційної політики для вирішення політичних, історичних, культурних, економічних і інших проблем вірменства;

6) концептуальна розробка національної «ноополітики» - мережевоцентричної системи, і формування на цій базі єдиного інформаційного і організаційного простору вірменства [282].

Інформаційна політика Вірменії пережила значних змін. Обмеження роботи ЗМІ під час президентських виборів 2008 р., яке вплинуло на інтернет-ресурси новин і сайти опозиції, сприяло розвитку блогів і соцмереж. Висвітлення парламентських виборів 2012 р. було значно більш різнобічним, проте насьогодні прояви жорстокості і погрози на адресу журналістів сприяють самоцензурі. Як платформа для комунікації і координації політики в ІКТ і нормативноправовій сферах у Вірменії створена Рада з підтримки розвитку сектора ІКТ, консультативна група, яка складається з представників приватного сектора, чиновників і представників громадянського суспільства, і очолює його прем'єрміністр. Рада сприяє змінам політики та законодавства, у напрямку розвитку кіберпростору Вірменії та лібералізації радіочастотного спектру. Рада істотно спростила елементи процесу мережевого ліцензування. У Вірменії практикується ліберальний підхід щодо управління інтернетом. В країні проголосували проти поправок до Регламенту міжнародного електрозв'язку, запропонованих Росією і підтриманих державами-однодумцями на Всесвітній конференції з міжнародного електрозв'язку в грудні 2012. Ці поправки були спрямовані на передачу контролю над управлінням глобальною мережею Організації об'єднаних націй і, в результаті, на зонування кіберпростору. Вірменія була однією з перших пострадянських держав, в якому пройшла приватизація телекомунікаційної індустрії. Провайдери телекомунікаційних послуг значною мірою зосереджені в руках іноземних компаній. Уряд Вірменії ще в 2001 р. сформулював план розвитку сектора ІКТ. Паралельно був схвалений пакет поправок в законодавство, які звільняли ІТ компанії з персоналом до 15 осіб від прибуткового податку (20%) на три роки з моменту

заснування. Законопроект також передбачав пільгову ставку прибуткового податку для працівників ІКТстартапів на рівні 10 % замість загальнодержавного мінімуму, що становить в даний час 24,4% [271]. Уряд і міністерство економіки продовжують просувати розвиток сектора ІКТ, одночасно працюючи над розвитком електронного уряду в Вірменії і підвищуючи якість послуг зв'язку. Телебачення залишається основним джерелом інформації. Однак стрімко розвивається взаємодія через соціальні мережі. Лідирують Однокласники, Facebook на другому місці, але існує також і кілька локальних платформ соціальної взаємодії, найбільш популярна - це Hayland, що нараховує 156 000 зареєстрованих користувачів.

У 2013 р. платформа отримала фінансові вливання і була оновлена, щоб краще відображати «етнічні і психологічні характеристики Вірменського народу». Проте, соцмережі Facebook і Однокласники, також доступні на вірменській мові і підривають конкурентоспроможність локальних соціальних мереж. Ці сайти не тільки володіють високим проникненням, але вони також дозволяють отримати кращий доступ до членів вірменської діаспори, що є вважливим для внутрішньої і зовнішньої політики Вірменії. Соцмережі мають все значніший вплив на політичне життя. В ході парламентських виборів 2012 р., Facebook виступив як важлива платформа діалогу і ведення передвиборної кампанії, більшість політиків і їхніх партій вже були присутні в мережі. На думку Т. Кочаряна, блогера і експерта з інформаційної безпеки, політики все більше усвідомлюють, що інтернет, платформи соціальної взаємодії і блоги є важливими джерелами інформації для молоді, не в останню чергу через недовіру останніх до телебачення і газет [271]. Вірмени активно використовують простір інтернету для просування локальних громадських ініціатив. При цьому аудиторія, на яку розраховані ініціативи, знаходиться не лише всередині країни, а й і за кордоном. Члени діаспори, особливо що знаходяться в Каліфорнії, беруть помітну участь у політичній і фінансовій життя Вірменії.

З цієї причини основна частина контенту генерується вірменською та англійською мовами. В ой же час, мають місце злочини в мережевому просторі, за оцінкою поліції 80% кіберзлочинів в Вірменії відбуваються в соціальних мережах, серед яких найбільш поширені - розкрадання персональних даних та вимагання. Порушники часто створюють підроблені аккаунти і розміщують компрометуючі фото, наклепницькі заяви або пропонують сексуальні послуги від імені сфальсифікованих акаунтів з викраденими даними. Найчастіше злочинці дають реальні телефонні номери жертви, а компрометуючі матеріали видаляють тільки після отримання грошей.

Кіберзлочини в Вірменії часто пов'язані з невирішеним конфліктом з Азербайджаном через Нагірний Карабах. Експерти оцінюють це протистояння як інформаційну війну другого покоління. Конфлікт супроводжується втручанням третіх сторін, зокрема, свої інтереси в інформаційнішому протистоянні мають країни регіону – Турція, Іран, Грузія, а також глобальні гравці – РФ, США і ЄС. При цьому використовуються широко методи інформаційного впливу (пропаганда), а також кібератаки. Атаки на сайти загострюються в певні періоди р., часто в місяць здійснюється від 50 до 100 атак на вірменські сайти. За даними фонду «Нораванк»[271], вірменського аналітичного центру, який вивчає проблеми інформаційної безпеки, вірменські сайти часто атакують під час національних свят. Азербайджану в останні роки була властива багатоговекторна зовнішньополітична модель, хоча ситуація з демократизацією суспільства та правами людини і надалі залишається проблемною, про що свідчить аналітика незалежних експертів багатьох міжнародних організацій – Amnesty, Reporters sans frontières, Freedom House. Інформаційну політику характеризує комбінація цензури, електронного нагляду і фізичного впливу на громадян-дисидентів і незалежні засоби масової інформації. В країні відсутня свобода слова, всі провідні ЗМІ залишаються під контролем уряду, держава є власником 80 % газет в країні. Відомі випадки юридичного тиску, наприклад, у вигляді судових позовів за наклеп і дискредитацію, також при першій-ліпшій можливості застосовується до

незалежних ЗМІ. Інтернет часто виявляється єдиним альтернативним простором для вільного самовираження, але й інтернет все більше зазнає тиску Нормативно-правова база Азербайджану є продовженням законодавства радянського періоду. Держава реалізує свій вплив на сектор ІКТ шляхом підтримки тісних зв'язків з головним оператором країни, компанією «Delta Telecom» - найбільшим оптовим інтернет-провайдером, який контролює основну частину міжнародних з'єднань і керує єдиною точкою обміну трафіком інтернет. Міністерство зв'язку та високих технологій Азербайджану наділено значними владними повноваженнями, що дозволяє обмежувати, модифікувати і 327 здійснювати моніторинг інтернету в країні. З урахуванням відносин між інтернетпровайдерами та органами влади, офіційний Баку забезпечений неофіційними і неконтрольованими інструментами здійснення контролю над сектором ІКТ. Нафтозалежна економіка Азербайджану останні роки суттєво постраждала від падіння цін на нафту та зниження курсу її валюти, манату, на половину вартості. Тому нова концепція розвитку, під назвою «Азербайджан 2020: бачення майбутнього», робить акцент на економіці, заснованій на знаннях, і на проникненні ІКТ в усі сфери суспільства. Доступ до ІКТ і інфраструктура сконцентровані в містах, де знаходиться 80 % усіх стаціонарних мереж. Більш того, поширення стаціонарних мереж дещо зросла протягом останніх кількох років, досягнувши 18 %. Азербайджанці добре представлені в соцмережах і дуже активні в місцевій блогосфері. Переважає Facebook, де зареєстровано близько одного мільйона аккаунтів.

Досвід Арабської Весни спонукала азербайджанських активістів організувати власну Бакинську Весну в 2011 р., вимагаючи демократичної реформи і поваги до людських прав. Спочатку задумана як виключно онлайн-захід, учасники якого могли повідомляти про свою підтримку, поставивши 'Like' (що вже було для Азербайджану досить сміливим політичним кроком), акція трансформувалася в живий протест, призначений на 11 березня 2011 р.. У відповідь на Бакинську Весну розпочались арешти, кількість затриманих учасників в протестах, організованих за допомогою соціальних мереж,

становили сотні. Проте використання інструментів Web 2.0 азербайджанськими активістами не лише не припинився, а й набув нових форм. Так, наприклад, на початку 2013 р. в Баку за допомогою Facebook були організовані протести у відповідь на смерть призовника Д. Губадова, який, очевидно, загинув від поранень, отриманих під час 328 жорстокого конфлікту, пов'язаного з «дідівщиною». Сторінка в мережі Facebook «Зупиніть загибель солдатів», закликала приєднатися до протесту, призначеного на 12 січня. Протягом декількох днів "like" на сторінці поставили понад 17 тисяч користувачів, і близько 3000 взяли участь в акції протесту. Після участі в заході від 22 активістів вимагали заплатити штраф в розмірі зарплати за 1-2 місяці. У Facebook була запущена кампанія під назвою «5 qepik», з метою допомогти активістам виплатити штрафи; суть кампанії полягала в тому, щоб кожен «донор» пожертвував всього п'ять центів. Через п'ять днів вдалося зібрати більше 10 тисяч доларів, чого цілком вистачило для виплати штрафу. Декілька разів уряд робив спроби обмеження доступу до мережі інтернет. В 2013 р. члени уряду були стурбовані підвищенням активності в соцмережах і можливими у зв'язку з цим протестами перед виборами намагалися зробити це шляхом закриття інтернет-кафе регіонах в Ісмаил та Нахічеван. Іншим способом обмеження онлайн-активізму є обмеження вільного потоку інформації, блокуючи доступ до веб-ресурсів. У дні, що передували протестам 12 січня 2013 р., в зв'язку з загибеллю Д. Губадова, кілька веб-сайтів, які критикують уряд, включаючи azadliq.az, azadliq.org, musavat.com, qafqazinfo.az, повідомили про успішні DDoS- атаки на них. З законодавчої точки зору в Азербайджані, онлайн-контент відноситься до ЗМІ. Весь створюваний користувачами контент, від блогів до постів в мережі Facebook, відповідно підлягає законодавчому регулюванню як ЗМІ. Це звужує простір для політичної онлайн-активності та обмежує свободу слова і самовираження в віртуальному просторі. Має місце посилення контролю над цифровим простором і паралельне посилення урядового втручання в діяльність традиційних та нових ЗМІ. Важливою рисою азербайджанського інформаційного і мережевого

просторів є націоналізм. Політична криза в стосунках з Вірменією в зв'язку з невирішеним Нагірно-карабахським конфліктом провокує конфлікти між хакерами обох сторін. Націоналісти з обох сторін періодично завдають кібератаки на сайти супротивників і обмінюються один з одним образами в Мережі. Мають місце кібератаки на урядові сайти, ресурси ЗМІ, що критикують існуючий режим. Окрім 329 того, у цьому конфлікті задіяні ще декілька країн, які також мають свої інтереси в інформаційному та кіберпросторі. Наприклад, у січні 2012 р. Азербайджанська Кіберармія, група, ймовірно пов'язана з Іраном, атакувала приблизно 40 державних структур в знак протесту проти тісних відносин Баку і Тель-Авіва. Встановлено, що 24 з 25 були здійснені з Ірану, а одна - з Нідерландів. Значною проблемою також залишається онлайн-нагляд за громадянами, що здійснюється в інтересах влади Азербайджану. Вираз незгоди чи критика державних осіб в мережі часто призводить до відстеження автора. У повсякденному житті азербайджанці перебувають під враженням, що за їх діяльністю в інтернеті постійно спостерігають. Це призводить до значної самоцензури і страху, а отже виключає можливість демократичних процесів з використанням новітніх технологій, як-то участь в онлайн-дискусіях на «гарячі» політичні теми.

В 2013 р., в підтримку комплексного плану дій щодо запобігання випадків помилкової інформації про тероризм, була введена мобільна реєстрація. Всі мобільні пристрої повинні бути зареєстровані відповідно до свого ідентифікаційним кодом IMEI, SIM-картою та номером мобільного мережі з реєстрацією центру мобільних пристроїв. Органи безпеки мають доступ як до даних операторів мобільного зв’язку, так і до інтернет-проавайдерів. Програма «Uppdrag Granskning» («Місія - розслідувати»), шведське телешоу, яке займається розслідуваннями, в 2012 р. документальний фільм про телекомунікаційної компанії «TeliaSonera», фінськошведської фірми й основному акціонерові в «Azercell». У цьому документальному фільмі стверджувалося, що «TeliaSonera» дозволила встановити «чорні ящики» в своєму обладнанні, зробивши можливим моніторинг в реальному часі за

допомогою всіх форм комунікації в своїх мережах, включаючи геолокацію. Один абонент «TeliaSonera» в ході інтерв'ю заявив, що його допитували органи безпеки після того, як він проголосував за Вірменію в конкурсі пісень «Євробачення» в 2011 р.[270]. Про рівень правозастосування говорить також і той факт, що перше в історії Азербайджану рішення про застосування законодавчого регулювання у сфері захисту авторських прав на програмне забезпечення було прийняте у вересні 2017 р.. Бакинський адміністративно-економічний суд №1 зобов'язав компанію ABC Telecom, яка продавала комп'ютери з встановленим неліцензійним програмним забезпеченням Microsoft, відшкодувати збитки компанії Microsoft [7].

Таким чином інформаційна безпека в системі міжнародної безпеки пройшла різні етапи становлення. В другій половині XX сторіччя міжнародні домовленості здебільшого стосувались забезпечення існування та розвиток інформаційного середовища бізнесу. На межі тисячоліть відбулися значні трансформаційні процеси в геополітиці і внаслідок подвійної трансгранично-національної природи кіберпростору [128] національна політика держав щодо інформаційної безпеки стає значимою у вимірі зовнішньої політики, оскільки пов'язана з розбудовою інфраструктури. І, очевидним є, що опрацювання міжнародних домовленостей в сфері інформаційної безпеки в цілому, і людини зокрема, значною мірою залежить від політичної волі держав, які мають та/чи змагаються за визначальний геополітичний вплив. На сьогодні, до таких держав, насамперед, належать США, Російська Федерація, КНР та ЄС. На сьогодні у світі сформувалось два основних підходи щодо змісту міжнародної інформаційної безпеки. Перша група країн демонструє підхід до проблематики міжнародної інформаційної безпеки в широкому розумінні , в основу якої мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір. Друга група країн звужує питання міжнародної інформаційної безпеки до міжнародної кібербезпеки і такий підхід зосереджується на боротьбі із злочинами у сфері інформаційно-комунікаційних технологій, в т.ч. боротьбу із кібертероризмом. Як наслідок, при цих підходах

простежується різне розуміння місця інформаційної безпеки людини в складній системі інформаційної безпеки як на міжнародному, так і на національному рівнях. Перший підхід, на нашу думку, передбачає узаконення значного простору для обмеження інформаційних прав і свобод людини на користь гарантування інформаційного безпеки міжнародної спільноти і окремих держав. При цьому, прихильниками такого розвитку міжнародної політики виступають здебільшого держави, що мають значні проблеми щодо реалізації конституційних засад демократії, або ж взагалі не визнають демократичних цінностей. Другий підхід визначається значно більшим соціальним і економічним спрямуванням, передбачає встановлення міжнародних стандартів для інформаційних прав та свобод людини (особливо пов'язаних з використанням мережі) на достатньо високому рівні. При цьому не передбачає втручання в питання інформаційного суверенітету, ведення інформаційних воєн та деякі інші аспекти політичної і військової сфери. Безперечною вбачається цінність напрацювання міжнародних стандартів як орієнтирів для підвищення рівня захисту прав і свобод людини в інформаційній сфері. Водночас, як свідчить аналіз становлення інституту прав людини у складі міжнародного права, їх значення здебільшого є прогностичним і полягає у виконані таких функцій як: визначають перелік прав та свобод, які відносяться до категорії основних та обов'язкових для всіх держав-учасниць відповідних міжнародних угод або конвенцій; формулюють головні риси змісту прав та свобод, які повинні втілюватись у відповідних конституційних та інших нормативних положеннях окремих держав; встановлюють зобов'язання держав щодо визнання та забезпечення проголошених прав та свобод, а також встановлення на міжнародному рівні гарантій, необхідних для реалізації і захист. прав та свобод; фіксують умови щодо застосування прав та свобод людини, одночасно із законними обмеженнями цих прав та свобод [256,с.359]. Як свідчить досвід країн з розвиненою демократією, інформаційна безпека людини не повинна протиставлятись інформаційній безпеці держави та суспільства. Адже саме людина визнається основною цінністю кожного суспільства і забезпечення її

прав і свобод є кінцевою метою реалізації функцій держави. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держав, попередження міжнародних конфліктів чи/та терористичних актів, а також забезпечення безпеки національних інформаційних ресурсів.

Таким чином, має місце конфлікт інтересів різних об'єктів інформаційної безпеки. Вирішення цього конфлікту демократичним шляхом є однією з первинних задач при створенні відповідних правових норм. Як бачимо, підходи США і ЄС до вирішення цього питання суттєво відрізняються. Про це свідчить як аналіз законодавства, так і правозастосування. США декларує високі стандарти прав і свобод людини в інформаційній сфері, але при виникненні протиріч між гарантуванням дотримання цих стандартів і інтересами національної безпеки перевага віддається саме інформаційній безпеці держави. Країни ЄС, в свою чергу, демонструють більш послідовну політику щодо гарантування і дотримання прав і свобод людини в інформаційній сфері. Про це свідчать, зокрема, останні зміни в законодавстві щодо захисту персональних даних. Окрім того, політика ЄС у інформаційній сфері характеризується узгодженістю і забезпечується дієвими механізмами реалізації.

Значну роль нормотворчості відграють міжнародні судові органи, зокрема суд ЄС та ЄСПЛ, які шляхом правозастосування конкретизують розуміння змісту правових норм на основі суспільної практики, а часом і формують нове розуміння з огляду на зміни, що відбуваються в суспільстві. Зокрема, про це свідчить аналіз рішень у справах ЄСПЛ щодо права на доступ до інформації, який відображає зміну розуміння цього права, а також його співвідношення з іншими інформаційними правами, зокрема правом на захист персональних даних, свободою вираження поглядів тощо. Україна, обравши шлях євроінтеграції і підписавши угоду про асоціацію з ЄС взяла на себе зобов'язання щодо адаптації законодавства з відповідними нормами ЄС. Відповідно, значні зусилля спрямовуються власне на приведення у відповідність вже існуючого законодавства. Проте самих змін в законах не

достатньо. Правове регулювання має відображати бажані соціальні зміни і їх стимулювати. Як вже неодноразово звертали увагу, загрози інформаційній безпеці людини значною мірою узалежнені від геополітики. Аналіз ситуації в країнах Східного партнерства, зокрема досвід Грузії, Вірменії і Молдови в сфері інформаційної безпеки людини є цінним для України з огляду на: (1) проевропейську політичну спрямованість, а отже і спроби адаптації до законодавства і стандартів ЄС; (2) геополітичну ситуацію, що пов'язана зі значним впливом (в т.ч. інформаційним) зі сторони Російської Федерації; (3) наявність територій, що не підконтрольні уряду, і використання конфліктів в цілях підривання суверенності державної влади; (4) нестійку політичну і економічну ситуацію в середині держави. На пострадянському просторі сьогодні простежується виокремлення двох груп країн, що різко відрізняються принципами формування політики у інформаційній сфері. Про це свідчать також результати опитування 50 експертів ІКТ, які відображені в дослідженні «Ціна свободи і безпеки. Індекс ІКТзаконодавств Євразії за 2016 р. », виконаному DR Analytica на замовлення Digital.Report.[497] У першій групі опинилися Вірменія, Грузія і Молдова: націленість влади цих країн на збільшення свободи у всіх сферах, а також облік економічного ефекту від вжитих заходів дозволяє проводити збалансовану політику, одночасно приводить до збільшення безпеки. Так, зокрема, в Молдові прийняті в 2016 р. правові акти збільшували як свободу, так і безпеку в усіх сферах. Друга група країн, до якої входять Білорусь, Азербайджан, Росія, Казахстан і Киргизстан, в інформаційній політиці віддає пріоритет інтересам безпеки, переважно - державної. Така політика веде до обмеження свободи інформації для особистості і суспільства. Ці країни також беруть за основу реалізовані в Росії законодавчі ініціативи, зокрема, ті закони, що пов'язані з моральною стороною інтернет-контенту, а також з інформаційною безпекою держави. Проблемним питанням в країнах пострадянського простору залишається боротьба з кіберзлочинністю. Хоча в більшості країн ратифікована Конвенція про кіберзлочинність та прийняті відповідні закони по боротьбі з кіберзлочинністю,

реалізація їх положень зачасту є малоефективною, зокрема через те, що влада не вважає кіберзлочинність реальною загрозою, якщо вона не загрожує безпосередньо їх режиму або економічним інтересам.

Таким чином, міжнародний досвід свідчить про дихотомію проблеми міжнародної інформаційної безпеки, та інформаційної безпеки людини як складової інституту прав людини в міжнародному праві. Узгодження основних питань є необхідним з огляду на економічні інтереси держав, демократичні цінності та глобалізаційні процеси, і, водночас, практично неможливим з огляду на розбіжності в інтересах основних геополітичних гравців. При цьому закладення правових основ інформаційної безпеки людини лише на національному рівні є недостатнім з огляду на глобалізацію, інтенсивні транскордонні інформаційні процеси, трудову міграцію, е-комерцію, втрату ідентичності та ще цілу низку соціальних процесів, що виникають у зв'язку зі становленням глобального інформаційного суспільства.

РОЗДІЛ 3.
ПРІОРИТЕТИ РОЗВИТКУ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СУСПІЛЬСТВІ

3.1.Шляхи формування сучасної державної політики щодо інформаційної безпеки в Україні

Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави» [207]. Окрім того, в ст. 17 було закріплено забезпечення інформаційної безпеки як одну з найважливіших функції держави і справу всього Українського народу. Відповідальність за забезпечення державного суверенітету, в тому числі інформаційного, здійснення внутрішньої і зовнішньої політики держави, виконання Конституції і законів України, актів Президента України статтею покладено на Кабінет Міністрів України. При цьому рішення, які приймаються суб’єктами державного управління, повинні відповідати положенням державної політики, а державна політика за жодних обставин не повинна виходити за межі законодавства. Проте, в умовах правової соціальної держави передбачається активне державне втручання в процес юридичного регулювання суспільних відносин, гарантування соціальних свобод, оскільки беруться до уваги так звані «неспроможності ринку», до яких традиційно відносять: суспільні блага, зовнішні ефекти, природні монополії та інформаційну асиметрію. В той же час слід зважати на обмеження державного втручання, так звані неспроможності влади. Це передусім проблеми, які є властивими прямій демократії: парадокс голосування, інтенсивність вподобань і пакетування позицій; представницькій владі: вплив організованих інтересів, географічні виборчі округи, обмежені часові горизонти, породжені виборчими циклами, позування перед громадськістю; бюрократичному 336 забезпеченню:

проблеми державних інститутів, труднощі оцінювання наданих послуг, обмежена конкуренція, захист прав державних службовців, бюрократичні ігри з державно-політичними рішеннями; децентралізації: розмиті повноваження, фіскальні зовнішні ефекти [71]. В глобалізованому сучасному суспільстві слід також зважати на взаємозв'язок і взаємопроникнення комерційних інтересів великих корпорацій і політичних сил. Підходи до розуміння інформаційної безпеки України та світу за цей час зазнали суттєвих трансформацій, зокрема, сформувались політичні уявлення про місце цієї сфери в суспільному житті, роль держави в її регулюванні, розуміння мети і змісту державного управління інформаційною безпекою, механізмів державного впливу на інформаційні процеси та відносини. Відповідним чином змінювалося законодавство, структура та функції суб'єктів цієї політики. За формальну основу дослідження державної політики інформаційної безпеки людини в Україні було взято періодизацію новітньої історії державного управління забезпеченням інформаційної безпеки України, яку здійснив Зозуля О.С. з урахуванням таких трьох критеріїв:

1) розвитку національного законодавства як правової основи державного управління;

2) структури та змісту діяльності суб'єктів забезпечення інформаційної безпеки в контексті еволюції теорії державного управління;

3) основних змін об'єкта управління (власне інформаційної безпеки). Хоча, здійснення державної політики інформаційної безпеки як окремого напряму, на нашу думку, не може розглядатись на перших трьох етапах.

І лише починаючи з 2014 р. можна простежити тенденції до формування цього напряму. Нижче зміст окремих етапів державної політики у сфері інформаційної безпеки людини з урахування предмета нашого дослідження, а також з огляду на здійснене дослідження становлення нормативно-правового забезпечення інформаційної безпеки людини в Україні.

На першому етапі (1991-1997 рр.) пріоритетним завдання було формування сукупності інститутів державної влади, що забезпечуватимуть

прямий державний контроль та різновекторний вплив на інформаційний простір України, а “інформаційна безпека” як окрема самостійна категорія ніде не визначалася. Від СРСР Українська держава успадкувала модель адміністративно-державного 337 управління, відома у англомовному середовищі як “Old Public Management”. Її особливостями, насамперед, є: ієрархічний, вертикально інтегрований спосіб організації системи управління, з чітким розмежуванням повноважень, субординацією для різних рівнів органів і посадових осіб; прямий (адміністративний) державний контроль за всіма сферами життєдіяльності; відокремленість і закритість влади від суспільства[156]. Окрім того, створена ще за радянських часів політична система гальмувала суспільний розвиток, вступала в суперечність з економічним базисом, особливо з інститутом приватної власності, а також Радянська концепція прав людини суттєво відрізнялась від концепції прав і свобод людини, яка була покладена в основу Хартії прав людини. Радянська держава і комуністична ідеологія розглядалися як джерело прав людини, а правова система СРСР використовувала право і закон як важелі політики, а суди як органи виконавчої влади. Свобода інформації та похідні від неї права суперечили ідеї комунізму, тому в правовому полі знайшлось місце категоріям «цензура», «атеїзм», «репресії», «терор», «інакомисліє» та іншим. Диктатура пролетаріату повинна була придушити опір інших класів, які марксизм розглядав антагоністичними до класу пролетаріату.

Одним із найболючіших питань радянської спадщини для України стало національне, хоча на той момент воно не стояло так гостро. Більшовики, проголошуючи на словах дружбу народів, інтернаціоналізм і вільний розвиток усіх націй і народностей, дотримувалися на практиці відомої марксистської тези про те, що пролетарі не мають національності, наслідками такої політики були голодомори, масові депортації та русифікація. Національна політика використовувалась задля «окозамилювання» - про що свідчить створення не тільки союзних, а й автономних республік, національних країв і областей, а також збереження аж до 1991 р. графи про національність у радянських

паспортах і наявність в офіційній радянській статистиці даних про національний склад населення СРСР і окремих союзних республік. В Україні, на відміну від країн Прибалтики та східноєвропейських держав, які раніше входили у так звану соціалістичну співдружність, не відбулося осмислення і, як наслідок, відторгнення радянської спадщини. Тому формування усіх напрямів державної політики пострадянського періоду розпочалось радянською партійно-номенклатурною «елітою» на звичним їм засадам. Після розпаду СРСР Україна фактично залишилась сам-на-сам зі своєю самостійністю - без будь-якого державного апарату.

У новій державі не було власної законодавчої гілки влади, розвинутого апарату судової влади, а апарат четвертої влади, тобто засобів масової інформації, був дуже слабенький. Найрозвинутішим виявився апарат виконавчої влади - Кабінету Міністрів, кадри якого досить швидко зорієнтувалися і проникли у нові сегменти інших гілок влади. Вони зосередилися в апараті законодавчої і судової гілок влади, а також підпорядкували інформаційне середовище. Тим не менш, важливими подіями цього етапу є створення Ради національної безпеки України в 1992 р. і прийняття Закону України “Про інформацію”, який визначив засади інформаційного суверенітету України, хоча сама категорія не визначалась. Натомість, в ст. 6 тогочасної редакції закону вперше для незалежної України було визначено поняття державної інформаційної політики як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації. Головними її напрямами і способами визначались забезпечення доступу громадян до інформації; створення національних систем і мереж інформації зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності; забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів; створення загальної системи охорони інформації; сприяння міжнародному співробітництву в галузі інформації і гарантування

інформаційного суверенітету України. На його основі в наступні роки було закладено правові основи державної політики у сфері ЗМІ шляхом прийняття законів "Про друковані засоби масової інформації (пресу) в Україні", "Про систему Суспільного телебачення і радіомовлення України", "Про Національну раду України з питань телебачення і радіомовлення», "Про державну підтримку засобів масової інформації та соціальний захист журналістів" та інші. Указом Президента України в 1994 р. на базі Державного комітету України у справах видавництв, поліграфії та книгорозповсюдження й Державного комітету України з охорони державних таємниць у пресі та інших ЗМІ було створено Міністерство України у справах преси та інформації [380], з доволі широким колом повноважень щодо державного управління в сфері забезпечення інформаційної безпеки України.

В цей же період в Концепції (основи державної політики) національної безпеки вперше в українському законодавстві було задекларовано, що загроза інформаційної експансію іноземних держав є однією з основних загроз національній безпеці України в інформаційній сфері [367]. Згодом з'ясувалося, що такі підходи призвели до загрозливих деформацій вітчизняного інформаційного простору, оскільки переважна більшість новостворених телерадіоканалів, газет, журналів, а також неурядові аналітичні 340 центри не підконтрольні державі, бо фінансуються фондів міжнародних донорських агенцій. Саме їх зусиллями в українське суспільство вносились непритаманні для вітчизняної цивілізаційної моделі ідеологія й цінності, організаційні моделі, просувалися певні ідеологеми, що негативно впливають на суспільну думку щодо проблем внутрішньої та зовнішньої політики тощо [154].

Знаковими на цьому етапі було ще дві події - Конституційним Судом України під час розгляду справи щодо офіційного тлумачення ст. 3; 23; 31; 47; 48 Закону України "Про інформацію" було винесено рішення, що в Україні поняття "інформаційна безпека" законодавчо не визначено [45], а також створення Комісії з питань інформаційної безпеки [66]. Важливим для цього етапу було також усвідомлення існування різних моделей розробки державної

політики. Типова для радянського періоду модель "зверху - вниз", яка передбачала, що державні рішення приймаються на вищих рівнях державного управління, а низові рівні є пасивним виконавцями політики, перестає бути єдино можливою. Хоча, на нашу думку, на цьому етапі ще зарано говорити про закладення основ моделі "знизу - вгору", яка передбачає, що формування державної політики починається з низових структур управління при активному залученні громадян, громадських інститутів. Адже для політичної системи України того періоду були притаманні застиглість і обмежена спроможність до трансформацій, монополія з боку кланової бюрократії, продажність і корупція, відсторонення від політичного життя широких верств населення, контрольованість засобів масової інформації, тотальна цензура, висування на керівні політичні посади осіб, професійно не підготовлених, схильних до хабарництва, але відданих тому хто їх фінансує і, зачасту, пов’язаних з ним сімейними зв’язками, бізнесовоми, а часом і злочинними інтересами. Неможливо переоцінити значення закріплення в Конституції України інформаційних прав, а також проголошення забезпечення інформаційної безпеки України "справою всього українського народу". Таким чином, інформаційна безпека з вузькоспеціалізованого кола вжитку фахівців прикладного характеру була піднесена до правового закріплення на рівні Основного Закону. Як можна простежити, в науковій думці того періоду спостерігалось значне ототожнення понять «інформаційна безпека», «безпека інформації», «захист інформації», що й досі має місце в багатьох країнах [83]. Для питання, що досліджується, має значення п. 5 ст. 92 Конституції України, де закріплено, що виключно законом встановлюються засади організації транспорту та зв’язку, а також основи національної безпеки, складовою якої слід вважати інформаційну безпеку. Забігаючи наперед, слід звернути увагу, що все ще не прийнято закону, який би визначав концепцію державної інформаційної політики України. Хоча відбулося декілька спроб ухвалити концепцію державної інформаційної політики на законодавчому рівні – 2002, 2009, 2010 та 2011 рр.

Поруч із закріпленням інформаційної безпеки як складової національної безпеки, Конституція України окреслила повноваження суб'єктів, що відповідають за формування і реалізацію відповідної державної політики - Президент України; Рада національної безпеки і оборони України; Верховна Рада України; Кабінет Міністрів України та інших. Початок другого етапу (1998-2005 рр.) автор пов'язує з прийняттям 4 лютого 1998 р. Закону України "Про Концепцію Національної програми інформатизації" [38], в якому "інформаційна безпека", визначена як невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки. Насамперед йшлося про політику інформатизації, про яку Арістова І.В. зазначає, «Те, що називали "політикою інформатизації" означало таку політику, що орієнтована на створення техніко-технологічної бази переходу країни до інформаційного суспільства ("залізо", "кабелі", будинки і т.ін., тобто взагалі — предмети матеріальні). У політиці не було місця для вирішення проблем інформаційних прав особистості, узгодження інтересів людини — суспільства — держави. Можна говорити про те, що ця політика прагнула "уникнути" соціальних проблем, зокрема, впливу інформації на громадську свідомість, демократизацію суспільства.»[15]

Проте, як зазначає професор, ця політика прагнула "уникнути" соціальних проблем, зокрема, впливу інформації на громадську свідомість, демократизацію суспільства. Як вже зазначалось в ці роки ознаменувались прийняттям низки правових актів задля врегулювання інформаційної сфери, і ще більшою кількістю спроб законодавчо визначити поняття "інформаційний суверенітет" і "інформаційна безпека", жодна з яких так і не було легалізовано. Разом з тим Рада національної безпеки і оборони України у рішенні "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України", звертала увагу на незадовільний стан забезпеченні інформаційної безпеки України і поставила низку завдань відповідним міністерствам і відомствам у сфері забезпечення інформаційної безпеки України, тм самим визначивши по суті систему органів, що здійснюють

забезпечення інформаційної безпеки. Кабінету Міністрів України було доручено: розробити проект Концепції національної інформаційної політики та інформаційної безпеки України; розробити заходи щодо оптимізації системи державних органів, які реалізують інформаційну політику, забезпечивши чітке розмежування повноважень і налагодження їх взаємодії та координації; створити організаційну структуру системи забезпечення інформаційної безпеки; визначити механізм реалізації повноважень Генерального штабу Збройних Сил України щодо участі в організації і контролі за інформаційним простором держави та його здійснення в особливий період; Службі безпеки України – подати пропозиції щодо вдосконалення роботи з протидії інформаційним агресіям та спеціальним інформаційно- пропагандистським операціям, здійснюваним проти України іноземними спецслужбами; новоствореній Міжвідомчій комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України – координація виконання заходів щодо забезпечення формування і захисту національного інформаційного простору, безпеки у цій сфері, розроблення і підготовка проектів відповідних нормативно-правових актів. Абсолютно новим для України кроком щодо захисту власного інформаційного простору та гідного представлення у міжнародному інформаційному просторі стало затвердження "Державної програми забезпечення позитивного міжнародного іміджу України на 2003-2006 роки" 15.10.2003 р., якою передбачалось вироблення єдиного комплексного підходу до формування та здійснення інформаційно-пропагандистської політики держави, яка б охоплювала 343 різноманітні сторони її життя [357].

Однією з найважливіших подій цього етапу стало прийняття у 2003 р. Закону України "Про основи національної безпеки України", що визначив загальну структуру суб'єктів та об'єктів національної безпеки, встановив основні напрями розвитку політики державної безпеки [76]. Ще однією інституцією, що повстала на цьому етапі є Національна експертна комісія України з питань захисту суспільної моралі, як постійно діючий державний

позавідомчий експертним і контролюючим органом, який діє відповідно до Закону України „Про захист суспільної моралі” № 1296-IV від 20 листопада 2003 р. та Положення про Національну експертну комісію України з питань захисту суспільної моралі, затвердженого постановою Кабінету міністрів України №1550 від 17 листопада 2004 р..

Вона проіснувала до 2015 р.. Основними завданнями були: проведення експертизи продукції, видовищних заходів сексуального чи еротичного характеру та продукції, що містить елементи або пропаганду культу насильства, жорстокості, порнографії; аналіз процесів і тенденцій, що відбуваються у сфері захисту суспільної моралі, розроблення для органів державної влади та органів місцевого самоврядування рекомендацій з їх правового регулювання; контроль за дотриманням законодавства у сфері захисту суспільної моралі; участь у розробці міжнародних договорів України з питань захисту суспільної моралі. Діяльність Національної експертної комісії мала бути спрямована на піднесення культури та духовності українського народу, всіх національностей, що проживають на Україні, утвердження здорового способу життя та належного стану моральності в суспільстві, виховання майбутніх поколінь українців на основі традиційних духовних і культурних цінностей, уявлень про добро, честь, гідність, громадський обов’язок, совість, справедливість, на засадах народних традицій, українських звичаїв, етичних норм і правил поведінки, що склалася у суспільстві. Для реалізації цих завдань комісії було надано повноваження щодо проведення у межах своєї компетенції перевірок діяльності засобів масової інформації, юридичних осіб усіх форм власності, що займаються організацією видовищних заходів та діяльністю з обігу продукції сексуального чи еротичного характеру або такої, що містить елементи насильства і жорстокості. Рішення Національної експертної комісії, ухвалені в межах її повноважень, були обов'язковими для розгляду центральними і місцевими органами влади, засобами масової інформації всіх форм власності, а також фізичними та юридичними особами. В цей період було здійснено спробу дебюрократизації управлінської системи та

впровадження нових підходів до організації процесу державного управління з високим ступенем орієнтації на ефективність та результативність. В результаті такою інновацією стала модель “Нового державного управління” (New Public Management). Основний зміст нової моделі полягає у зміні принципів формування організаційної структури державного управління; підвищенні гнучкості прийняття рішень у державному апараті, зменшенні його ієрархічності, делегування повноважень на нижчий рівень прийняття рішень та посилення механізмів зворотного зв’язку між державою та громадянами [11, 271]. 3-й етап (2006-2013 рр.) Зозуля характеризує як етап кардинальних змін у державному управлінні інформаційною безпекою, інтенсивною роботою з визначення концептуальних засад системи забезпечення інформаційної безпеки в Україні, які мали базуватися на постулатах та цінностях громадянського суспільства, відповідати сучасним європейським нормам, упровадження яких розглядається як безпосередній обов’язок держави [156].

Ця позиція, на нашу думку, категорично не відповідає дійсності. Хоча, як наслідок участі у Всесвітньому Самміті Інформаційного Суспільства в січні 2007 р. і було прийнято Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 роки”, де законодавчо закріплено поняття “інформаційна безпека” [378]. Проте, його реалізація так і не стала пріоритетом в державній політиці. Про це свідчить і той факт, що Закон на 2007-2015 роки досі залишається чинним, наступної його редакції не існує і, наскільки нам відомо, не передбачається її створення найближчим часом. Про неадекватність реальним умовам, декларативність і неефективність, а подекуди – невідповідність політики інформаційної безпеки цього періоду національним інтересам держави і суспільства свідчить також інформаційне 345 противоборство та реальні військові дії на території України, якими увінчалась така політика. Хоча, мали місце певні поодинокі спроби. У 2009 р. підготовлена і затверджена Указом Президента України від 08.07.2009 р. № 514/2009 Доктрина інформаційної безпеки країни [121]. Доктрина окреслювала основні засади інформаційної безпеки України, визначила місце інформаційної

безпеки в системі забезпечення національної безпеки України, називала реальні та потенційні загрози інформаційній безпеці України, визначала напрями державної політики у сфері інформаційної безпеки держави. Слід згадати також Хартію про партнерство заради інформаційних прав і свобод та захисту суспільної моралі, підписану у 2009 р. [496]. Хартія за своєю формою і змістом є суспільним договором, що укладений суб'єктами інформаційного процесу та представниками державних органів України з метою запровадження саморегулювання в дотриманні суб'єктами інформаційної діяльності законодавства про захист суспільної моралі, яка є не тільки конституційним обов'язком Української держави, але й однією із найважливіших складових національної безпеки України. Наступним кроком стало схвалення у 2010 р. Концепції проекту Закону України "Про основні засади державної комунікативної політики" метою якої є визначення шляхів законодавчого врегулювання питання забезпечення взаємодії між органами державної влади, органами місцевого самоврядування, засобами масової комунікації і громадськістю на засадах рівноправного партнерства, що сприятиме зміцненню демократії, становленню громадянського та інформаційного суспільства [388]. В травні 2011 р. набула чинності нова редакція Закону України «Про інформацію», в ст. 3 якого серед основних напрямів державної інформаційної політики з'явились: «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; забезпечення інформаційної безпеки України та інші. Таким чином, забезпечення інформаційної безпеки було віднесено до напрямів реалізації державної інформаційної політики. При тому, що норма щодо її розробки і здійснення залишилась без змін - органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції, тобто, по факту, всі і ніхто конкретно. Важливим кроком щодо забезпечення інформаційної безпеки людини були ратифікація в 2010 р. Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою

персональних даних та Додаткового протоколу до неї, як наслідок - прийняття Закону України «Про захист персональних даних» і створення Державної служби України з питань захисту персональних даних.

Останній було надано широкі повноваження щодо реалізації державної політики у сфері захисту персональних даних, зокрема, контроль за додержанням вимог законодавства про захист персональних даних; реєстрація бази персональних даних та ведення Державного реєстру баз персональних даних; здійснення державного нагляду та контролю за додержанням законодавства про захист персональних даних та інші, всього понад 30 повноважень. Цей Закон, як і діяльність Служби зазнали суттєвої критики, що призвело до того, що в 2013 р. Верховна Рада України прийняла Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», яким з метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних, повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. У 2011 р. набули чинності Закон України «Про доступ до публічної інформації» та нова редакція Закону України «Про інформацію», які стали важливою сходинкою до забезпечення не лише свободи інформації, а й демократизації суспільства.

Законом «Про доступ до публічної інформації» було визначено :

1) порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації;

2) гарантії та принципи забезпечення права на доступ до публічної інформації;

3) суб'єктів відповідних відносин, їх права та обов'язки тощо. Окрім того, нова редакція Закону «Про інформацію» передбачає «право кожного на інформацію», визначивши при цьому одним із основних напрямів державної інформаційної політики «забезпечення доступу кожного до інформації». У ст.

20 цього ж Закону було закріплено важливий принцип максимальної відкритості, згідно з яким «будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом», та інші положення, важливі для реалізації права на доступ до інформації, а саме: дозвіл на поширення інформації з обмеженим доступом, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від поширення (ч. 1. ст. 29); визначення невичерпного переліку інформації, що становить предмет суспільного інтересу (ч. 2 ст. 29); звільнення від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно необхідною (ч. 3 ст. 30).

Таким чином, ці два закони демонстрували відмову від хибної концепції права власності на інформацію загалом і власності держави на інформацію зокрема. Вони закріпили підхід, що ґрунтується на Конституції України, Цивільному кодексі України та міжнародних стандартах і передбачає, що інформація є об'єктом особистих немайнових прав, об'єктом особистих прав фізичної чи юридичної особи. В 2013 р. було схвалено Стратегію розвитку інформаційного суспільства в Україні, що визначила мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні [388].

В Стратегії зазначається, що забезпечення інформаційної безпеки у процесі використання інформаційнокомунікаційних технологій є однією з найважливіших умов успішного розвитку інформаційного суспільства. Суттєвим недоліком цього документа, було акцентуація уваги на заходах по технічному забезпеченню інформаційної безпеки (захист інформації, забезпечення безпеки інформаційних мереж, тощо). 4-й етап (починаючи з 2014 р. – по теперішній час) в історичній динаміці становлення і розвитку системи забезпечення інформаційної безпеки України запропонованій Зозулею С.В. співпадає з періодизацією розвитку правового забезпечення інформаційної безпеки.

Кардинальна трансформація взаємодії між державою і громадянським суспільством призвела до запровадження нових способів і механізмів державного управління з метою 348 забезпечення ефективного управління суспільними процесами в сучасних умовах. Окрім того, проєвропейський вектор зовнішньої політики і підписання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі Угоди про асоціацію) [77] в державному управлінні намітився курс на запровадження європейської моделі належного (доброго) управління .

Першою реакцією на ситуацію, що склалась в Україні, стало Рішення Ради національної безпеки і оборони України “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” [363], а також було скасовано чинність низки актів РНБО затверджених Президентом України, в тому числі Доктрина інформаційної безпеки України, що була затверджена в 2009 р. [121]. На цьому етапі спостерігається суттєва інтенсифікація наукового опрацювання, публічної дискусії та нормотворчої роботи щодо питань забезпечення інформаційної безпеки. В 2014 р. до Верховної Ради України був поданий Проект Закону “Про засади інформаційної безпеки України” (реєстраційний № 4949 від 28.05.2014 р.) [354], Державним комітетом телебачення і радіомовлення України розроблено проект нової Доктрини інформаційної безпеки України і проект Стратегії розвитку інформаційного простору України на період до 2020 р.

В 2015 р. Верховна Рада України суттєво доопрацювала законодавство щодо доступу до публічної інформації, особливо слід виділити чотири закони. Перший стосувався внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних. Закон передбачив створення єдиного державного веб-порталу відкритих даних, а також встановив, що оприлюднена на такому веб-порталі інформація є публічною інформацією у формі відкритих даних 45 “Good Governance”. Концепція “Good Governance” наповнює державне управління гуманітарною та соціальною складовою,

формує новий підхід до розуміння врядування, яке має тепер відповідати не лише вимогам ефективності, але й бути відкритим, доступним, підзвітним і підконтрольним, а отже, чутливим до вимог громадян, їхніх потреб і запитів. Тобто це спосіб реалізації публічної влади, завдяки якому досягаються реальна участь громадян у виробленні та реалізації публічної політики; об'єднання потенціалу всіх трьох секторів (влада, бізнес, громадськість); постійний контроль різними інститутами громадянського суспільства за публічною владою [156] 349 та є дозволеною для її наступного вільного використання та поширення [77]. Беручи до уваги можливості, які відкриває цей закон перед громадськістю, значення його прийняття для подальшого розвитку українського суспільства і для кожної людини зокрема, важко недооцінити. Другий Закон України «Про внесення змін до статті 28 Бюджетного кодексу України щодо доступу до інформації про бюджетні показники у формі відкритих даних» передбачає оприлюднення бюджетних запитів, квартальної та річної звітності про виконання Державного бюджету України, паспортів бюджетних програм та звітів про виконання паспортів бюджетних програм, рішень про місцеві бюджети, інформації про виконання Державного бюджету України та місцевих бюджетів (крім бюджетів сіл і селищ)[304].

Прийнятий Закон України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 років» має за мету врегулювання основних засад, принципів, гарантій, шляхів реалізації державної політики щодо забезпечення доступу до архівної інформації репресивних органів. А Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» запроваджував механізм подання індивідуальних та колективних звернень в електронній формі[342]. В 2015 р. було затверджено нову Стратегію національної безпеки України [379], в якій пріоритетами забезпечення інформаційної безпеки визначені: 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; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; створення і розвиток інститутів, що відповідають за інформаційнопсихологічну безпеку, з урахуванням практики держав - членів НАТО; удосконалення професійної підготовки у сфері інформаційної безпеки. Як зазначає Зозуля О.С. насьогодні жоден з існуючих центральних органів виконавчої влади не в змозі самостійно здійснювати весь комплекс заходів із забезпечення інформаційної безпеки. Хоча в січні 2015 р. було утворено Міністерство інформаційної політики України, як головний орган у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України [311], проте інформаційний суверенітет України на законодавчому рівні не визначений. Була спроба ще в 1999 р. прийняти відповідний закон [361], але і досі це питання не вирішено. В 2015 р. було підписано “Дорожню карту програми Партнерства зі стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО” [124]. Програма Партнерства спрямована на здійснення комплексної підтримки України у сфері стратегічних комунікацій, зокрема протидії російській пропаганді та інформуванні громадськості про події в Україні. В 2016 р. було визначено принципи, пріоритети та напрями забезпечення кібербезпеки України в Стратегії кібербезпеки України[443]. І лише на межі 2016 і 2017 років держава нарешті отримала Доктрину інформаційної безпеки України [121], яка визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері, і спрямована на уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах

розв'язаної нею гібридної війни. Складно на даний момент оцінити вплив цього документу на українські реалії інформаційної сфери.

Передбачено, що основними суб'єктами повноважень згідно неї мають стати Кабінет міністрів, Міністерство інформаційної політики, Міністерство закордонних справ, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Служба безпеки України, розвідувальні органи, Державна служба спеціального зв'язку та 351 захисту інформації, Національний інститут стратегічних досліджень; а також РНБО як орган, що здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. Суттєво посилені і конкретизовані повноваження Міністерства інформаційної політики. Таким чином, можна констатувати, що чинне законодавство не дає цілісного і системного закріплення офіційних поглядів, принципів, напрямів діяльності, спрямованих на реалізацію державної політики інформаційної безпеки людини. Водночас, аналіз правових основ державної політики дозволяє зробити висновок, що як окремий напрям державна політика інформаційної безпеки (і в цілому, і людини, зокрема) не виділяється, хоча в науковій думці існує такий підхід (Олійник О.В., Зозуля О.С., Ліпкан В.М., Кормич Б.А). Б. Кормич відзначав, що як за суб'єктним складом, так і за компетенцією механізм інформаційної безпеки повинен дещо відрізнятися від традиційного механізму державного управління, що інституціональний механізм інформаційної безпеки являє собою сукупність інститутів публічної влади та інститутів громадянського суспільства, до компетенції яких входить вирішення питань щодо забезпечення умов функціонування і розвитку інформаційної сфери [208]. При цьому основні напрями забезпечення інформаційної безпеки він суттєво звужував, розглядаючи їх лише через сферу обігу інформації, тобто її одержання, зберігання, використання, поширення та захисту. Його критикує Олійник О.В. і гостро ставить питання про необхідність відмовитися від подальшої

примітивізації інформаційної безпеки як складової національної безпеки лише в інформаційній сфері, тобто сфері обігу інформації. Погоджуючись з його аргументацією, вважаємо доцільним концептуальний підхід до визначення інформаційної безпеки як складової національної безпеки у сфері інформаційної діяльності. Інформаційна безпека має бути важливою основою інформаційних складових усіх сфер забезпечення національної безпеки [288]. Якщо ж говорити про інформаційну безпеку людини, то політика щодо неї знаходиться на перетині декількох пріоритетних напрямів державної політики – насамперед, інформаційної політики, політики національної безпеки та політики з прав людини, але також і правової політики, соціальної політики, політики у галузі освіти і науки, і, навіть, зовнішньої політики. При цьому, за кожним напрямом має враховуватись єдиний підхід до забезпечення інформаційної безпеки людини – створення умов для своєчасного виявлення потенційних і реальних загроз; розробки і впровадження заходів і засобів попередження і протидії викликам; нейтралізації або послаблення дії небезпек. Тому вбачається доцільним визначити на рівні незалежного органу держави закріпити інститут Уповноваженого з інформаційної безпеки людини, як аналог прийнятого в ЄС інституту інформаційного комісара.

Його діяльність має бути спрямована реалізацію політики держави щодо забезпечення інформаційної безпеки людини, в тому числі захист прав і свобод людини в інформаційній сфері, зокрема, права на доступ до публічної інформації та захист персональних даних. Уповноваженому необхідно надати достатні важелі впливу, з однієї сторони, на формування інформаційного законодавства, наприклад, шляхом обов’язкової експертизи нормативних актів що зачіпають відповідні права людини, з іншої - повноваження щодо припинення правопорушень та відновлення порушених прав. Окрім того, ефективність політики держави щодо інформаційної безпеки людини значною мірою залежить від системного розуміння проблеми розбудови приязного для людини інформаційного суспільства, а отже вимагає визначення єдиного органу відповідального за її здійснення. З цією метою та з урахуванням

позитивного досвіду європейських країн, пропонується зосередити повноваження по реалізації політики держави щодо розбудови інформаційного суспільства в єдиному центральному органі виконавчої влади. При цьому, на законодавчому рівні має бути визначено відповідальність держави і зобов'язання щодо реалізації інформаційної політики у основних сферах життєдіяльності суспільства – обороні, захисті прав людини, економіці, освіті, охороні здоров'я, екології, демократизації та децентралізації тощо. Особливими сферами відповідальності такого органу мають стати: координація розбудови інформаційної інфраструктури держави; забезпечення умов для реалізації інтересів людини, суспільства і держави в інформаційному (в т.ч. кібер) просторі; координація діяльності інших державних органів в інформаційній сфері, забезпечення безвідмовної роботи об'єктів критичної інформаційної інфраструктури, створення умов для 353 формування належного рівня інформаційної культури населення, в тому числі, професійної підготовки населення в умовах розбудови інформаційного суспільства, сприяння розвитку ІТ галузі, забезпечення відкритості та прозорості діяльності влади, а також сприяння формуванню позитивного іміджу України як в середині держави, так і за її межами.

3.2. Механізми державного регулювання відносин у сфері інформаційної безпеки

Механізм правового регулювання як сукупність правових засобів, за допомогою яких держава здійснює правовий вплив на суспільні відносини, насамперед, має на меті осягнути бажаний для держави і суспільства результат. Таким чином, він по суті відображає пріоритети політики держави в означеній сфері правового регулювання. Теоретичні основі механізму правового регулювання закладені в працях С.С. Алексєєва, зокрема, його монографіях "Механізм правового регулювання в соціалістичній державі" і "Теорія права", де категорія "механізм правового регулювання" визначалась через правовий

вплив. Однак поняття механізму правового регулювання вужче, ніж поняття механізму правового впливу. Не кожні суспільні відносини урегульовано правом. Зокрема, не завжди підлягають правовому регулюванню процеси виробництва інформаційного продукту, хоча щораз частіше мають місце техніко-юридичні норми; за загальним правилом поза межі правового регулювання виведено особисте життя і релігійні відносини тощо. Сфера правового регулювання може об'єднувати лише відносини, що піддаються правовому регулюванню - конкретні, значимі відносини, що усвідомлюються людиною, і щодо яких може бути прийняте вольове рішення. Так, відносини, що на сьогодні становлять суттєву загрозу інформаційній безпеці і пов'язані із негативним інформаційним впливом на її психіку, часто складно включити в перелік тих, що усвідомлюються і піддаються правовому регулюванню. Проте, власне визначення механізму правового регулювання покликано встановити межі необхідного і можливого втручання 354 держави у суспільні відносини, що виникають у зв'язку з інформаційною безпекою людини. Оскільки інформаційна безпека є невід'ємною властивістю її об'єктів, то говорити про регулювання інформаційної безпеки немає підстав. Це також одна з суперечностей, що має місце при визначенні самої інформаційної безпеки як стану, адже стани не регулюються правом. В такому випадку правове регулювання може розглядатись лише як складова забезпечення інформаційної безпеки. Подібний підхід можна зустріти в роботах багатьох українських і зарубіжних науковців. Істотне значення для розуміння правового регулювання має його предмет чи сфера правового регулювання. Інформатизація та інші етапи становлення інформаційного суспільства обумовили формування категорії «інформаційна сфера» як предмету правового регулювання. Російська класик інформаційного права І.Бачило, предметом, що формує спеціальну галузь відносин, умовно званих інформаційними, визначала сукупність реально існуючих матеріалізованих результатів творчості і праці, втілених: 1) в інформації, при різноманітності форм її прояву, і сформованих на її основі інформаційних ресурсах, 2) засоби і технології роботи з інформацією

(інформаційних технологіях); 3) засоби і технології комунікації інформації по мережах зв'язку. На базі цієї тріади предметів формується нова галузь суспільних відносин, яка в системі права виділяється як самостійна галузь правового регулювання [35]. Глибокий і комплексний аналіз цієї категорії було здійснено українським вченим Барановим О.А. в монографії «Правове забезпечення інформаційної сфери: теорія, методологія і практика» [24]. Проаналізувавши доктринальні і нормативні визначення інформаційної сфери, вчений сформулював авторське визначення інформаційної сфери як сукупності інформації та інформаційних ресурсів, інформаційної інфраструктури, суб'єктів, що здійснюють оборот інформації, тобто її створення, поширення (передавання), зберігання, використання та знищення, та забезпечують цей оборот, суспільних відносин, які при цьому виникають, системи її правового забезпечення, а також інституційної системи державного управління та регулювання цією сферою [24]. Проте, суспільні відносини, що виникають у зв'язку з інформаційною безпекою людини не обмежуються лише інформаційною сферою. Інформаційна безпека людини, як вже визначалось раніше, є складовою будь-якого виду інформаційної безпеки – чи то держави, чи суспільства, чи міжнародного співтовариства, а також має місце у складі інших сфер безпеки – продовольчої, екологічної, економічної, соціальної тощо. Таким чином, недоцільно визначати предмет її правового регулювання виключно в межах інформаційної сфери. Він є значно ширшим, комплексним за своєю суттю, охоплює декілька предметних сфер. Слід також враховувати, що у світі склалось дві тенденції правового регулювання правовідносин у інформаційній сфері: використовувати за аналогією законодавство, що існує, при цьому створюючи нові норми лише щодо дійсностей, що повстають у зв'язку з всеосяжною інформатизацією; або творити нове комплексне інформаційне законодавство. Україна, як відомо пішла першим шляхом, що призвело до виникнення суттєвим дисбалансів у питаннях інформаційної безпеки і проблем як при нормотворчій діяльності, так і на стадії правозастосування. Як приклад, можна розглядати ситуацію з правовим

регулюванням суспільних відносин, що реалізуються за допомогою інтернету. На думку, М. Дворового, експерта Центру демократії та верховенства права, впродовж тривалого часу інтернет в Україні перебував поза межами правового регулювання [107]. У рейтингу Freedom on the Net, що створює міжнародна правозахисна організація Freedom House, до 2013 р. включно Україна вважалася країною з вільним інтернетом.

Після Революції Гідності рейтинг свободи інтернету в Україні погіршився, країна перейшла із групи "вільних" до групи "частково вільних" країн. Починаючи з 2014 р. на обговоренні у владних структурах почастішали проекти актів, спрямовані на врегулювання відносин, що реалізуються за допомогою мережі, які, водночас, подекуди містять норми, спрямовані на обмеження прав користувачів інтернету. Так, в жовтні 2017 р. було прийнято два Закони, що мають суттєве значення як для інформаційної сфери в цілому, так і для інформаційної безпеки людини, зокрема, це «Про основні засади забезпечення кібербезпеки України» та Закон «Про електронні довірчі послуги». Станом на кінець 2017 р. на розгляді парламенту перебувало ще три законопроекти, які можуть суттєво вплинути на стан свободи інтернету в Україні: проект Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю (№ 2133а від 19.06.2015); проект Закону про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері (№ 6688 від 12.07.2017); проект Закону про внесення змін до Закону України «Про захист прав споживачів» та деяких законодавчих актів України щодо заходів детінізації діяльності суб'єктів електронної комерції (№ 6754 від 17.07.2017). Як обґрунтування ініціатив наводились необхідність забезпечити інформаційну безпеку України в умовах війни та посилити захищеність авторського та суміжних прав. Проте, такий підхід продовжує усувати «точкові» недоліки за відсутності загальної концепції регулювання інформаційної сфери. Таким

чином, посилюється дисбаланс між забезпеченням інформаційної безпеки і свободою інформації, яка є основою демократії.

При цьому, сценарії які розглядаються для врегулювання інформаційної сфери, сприймаються по-різному в наукових, урядових, бізнесових колах, а також серед представників інститутів громадянського суспільства. Останні насамперед пильнують свободу слова і там, де це можливо, наполягають на саморегулюванні. Ділові кола, а це ІТ-компанії та медіа бізнес, зацікавлені в правовому забезпечення ринкових умов для їх діяльності. Влада, затиснута поміж реальністю інформаційної війни та бойових дій на сході України, задекларованим процесом євроінтеграції та зовнішнім тиском, політичними лобістськими інтересами, а подекуди і корупційними схемами, в черговий раз демонструє При цьому в аналітиці громадських діячів ці права здебільшого називають «цифровими», ми ж не погоджуємось з таким підходом, що обґрунтовано в розділі 3 цього дослідження. 357 невиваженість державної інформаційної політики. Щодо науковців – останні 3 роки спостерігається певна дихотомія. З одного боку, кількість наукових досліджень цієї проблематики постійно зростає, з іншого – академічна наука, в цілому, є під загрозою. Проте, це питання виходить за межі предмету дослідження. Необхідним вбачається наукове осмислення, громадське обговорення і подальше нормативне закріплення прийнятного і обумовленого реаліями українського суспільства і держави принципів правового регулювання інформаційної сфери з метою забезпечення інформаційної безпеки людини. Власне виходячи з цих основоположних засад може бути розмежовано відносини щодо інформаційної безпеки людини, які:

1) обґрунтовано і ефективно регулюються правом,

2) не регулюються правом, але в цьому є суспільна необхідність;

3) не регулюються і регулювання не вбачається доцільним та/або можливим.

Принципи правового регулювання мають відображати його основну мету - забезпечення безперешкодного руху інтересів суб'єктів до цінностей, тобто

гарантованість справедливого задоволення інформаційних потреб людини, в умовах її захищеності від шкоди або інших небажаних результатів для її гідності та вільного розвитку. В правовій системі діє ієрархія принципів, які можна уявити як взаємодію різних видів по вертикалі. Бачило І. виділяє такі групи принципів, як:

1) загальнонаукові;

2) конституційні принципи організації суспільства і державної системи;

3) загальні принципи правового регулювання;

4) принципи правового регулювання в конкретній галузі;

5) принципи правозастосування.

В цілях цього дослідження хочемо звернути увагу на дві останні категорії. Зважаючи на те, що системоутворюючим законом в інформаційній сфері є Закон України «Про інформацію», то слід звернути увагу на принципи інформаційних відносин, які визначені ст. 3: «гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя» [360]. В Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», який досі залишається чинним, було визначено, що «при створенні інформаційного законодавства слід керуватися загальними принципами Конституції України, а також базуватися на принципах свободи створення, отримання, використання та розповсюдження інформації; об'єктивності, достовірності, повноти і точності інформації; гармонізації інтересів людини, суспільства та держави в інформаційній діяльності; обов'язковості публікації інформації, яка має важливе суспільне значення; обмеження доступу до інформації виключно на підставі закону; мінімізації негативного інформаційного впливу та негативних наслідків функціонування ІКТ; недопущення незаконного розповсюдження, використання і порушення цілісності інформації; гармонізації інформаційного законодавства та всієї

системи вітчизняного законодавства»[374]. Запропонований підхід базується на дослідженнях російських теоретиків інформаційного права Копилова В.А. і Бачило І.Л. Доцінюючи їх внесок в розвиток науки інформаційного права, вважаємо доцільним і необхідним їх переосмислення з огляду на сучасний розвиток інформаційної сфери суспільства, а також на інформаційне противоборство і обумовлені ним загрози інформаційній безпеці людини, демократичного суспільства і української держави. Л. П. Коваленко, зазначає, що правове регулювання інформаційних відносин ґрунтується на принципах інформаційного права, під якими розуміють основні вихідні положення, що юридично пояснюють і закріплюють об'єктивні закономірності суспільних відносин, що проявляються в інформаційній сфері [195] І до них відносить наступні – пріоритету прав особи; вільного створення й поширення будь-якої інформації, не обмеженої українським законом (принцип свободи творчості й волевиявлення); заборони створення й поширення інформації, шкідливої й небезпечної для розвитку особистості, суспільства, держави; вільного доступу (відкритості) інформації, не обмеженої національним законом (право знати), або принцип гласності; повноти опрацювання й оперативності надання інформації; законності; інформаційно-правового регулювання; вилучення «відчуження» інформації в її власника, відповідальності за неправомірне використання інформації (її сутності); обігу інформації; двоєдності інформації і її носія; поширення інформації; організаційної форми та принцип екземплярності інформації. Як на нашу думку, такий перелік є надмірно деталізований і поєднує в собі не лише спеціальні, а й загально правові принципи. Вважаємо обґрунтованою думку Баранова О.А., що незважаючи на те, що всі дослідники відзначають важливість формування принципів інформаційного права, дотепер не сформульована єдина, стала точка зору на їх зміст [25].

В якості базового принципу інформаційного права вчений пропонує використовувати принцип забезпечення інформаційної безпеки з урахуванням того, що забезпечення інформаційної безпеки є одним з основних атрибутивних

властивостей систем, у тому числі соціальних. Цей принцип знайшов відображення в ст. 17 Конституції України: “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу”. Наступні принципи Баранов О.А. вважає похідними від цього базового принципу і до них відносить такі:

1. Свободи одержання і поширення інформації.

2. Об'єктивності, вірогідності, повноти і точності інформації.

3. Гармонізації інтересів особи, суспільства і держави в інформаційній діяльності.

4. Мінімізації негативного інформаційного впливу.

5. Мінімізації негативних наслідків функціонування інформаційних технологій.

6. Недопущення несанкціонованого поширення, використання і знищення інформації

7. Інформація виступає в якості об'єкту цивільних правовідносин.

8. Невідторгаємість інформації.

9. Єдність і різниця інформації і носія інформації.

10. Об'єктність надання інформації.

11. Первинність створення інформації.

12. Обмеження доступу до інформації.

13. Обов'язковість опублікування.

14. Взаємна гармонізація інформаційного права і всієї системи вітчизняного законодавства.

15. Гармонізація українського інформаційного законодавства з міжнародним законодавством і законодавством інших країн [25]. Слід зважати, що сформульовані 2006 р. принципи інформаційного права України О.А. Баранов пропонував використовувати, насамперед, у процесі формування власне інформаційного законодавства, а також у процесі правозастосування існуючих правових норм, що регулюють інформаційні відносини. Також

звертав увагу на те, що сформована система принципів інформаційного права не є остаточною, тому що в діалектичному процесі створення конкретних правових норм інформаційного законодавства і розвитку загальної системи права держави, правосвідомості в Україні принципи можуть піддаватися відповідним змінам, як по кількості, так і по змісту. Погоджуючсь в основному з запропонованим підходом, зробимо спробу співставити запропоновану систему принципів з принципами правового регулювання у сфері інформаційної безпеки. О.В. Олійник вважає, вихідними положеннями формування і функціонування системи інформаційної безпеки як системоутворюючого фактору всіх складових національної безпеки, норм і правил поведінки громадян, державних і суспільних інститутів України у цій сфері, є наступні: пріоритет прав, свобод і законних інтересів людини і громадянина; верховенство права, рівність усіх суб'єктів правовідносин перед законом; відповідальність держави перед людиною за свою діяльність; комплексний підхід до вирішення завдань забезпечення інформаційної безпеки; єдність і взаємозв'язок напрямів забезпечення інформаційної безпеки; розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки; участь у міжнародних і регіональних системах інформаційної безпеки; оперативність, своєчасність, превентивність і адекватність заходів щодо попередження і захисту від зовнішніх інформаційних загроз та нейтралізації джерел внутрішніх інформаційних загроз [290, с.72]

Як свідчить досвід країн з розвиненою демократією, інформаційна безпека людини не повинна протиставлятись інформаційній безпеці держави та суспільства. Адже саме людина визнається основною цінністю кожного суспільства і забезпечення її прав і свобод є кінцевою метою реалізації функцій держави. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держав, попередження міжнародних конфліктів чи/та терористичних актів, а також забезпечення безпеки національних інформаційних ресурсів.

Таким чином, має місце конфлікт інтересів різних об’єктів інформаційної безпеки. Вирішення цього конфлікту демократичним шляхом є однією з первинних задач при створенні відповідних правових норм. Як було зазначено, підходи США і ЄС до вирішення цього питання суттєво відрізняються. Про це свідчить як аналіз законодавства, так і правозастосування. США декларує високі стандарти прав і свобод людини в інформаційній сфері, але при виникненні протиріч між гарантуванням дотримання цих стандартів і інтересами національної безпеки перевага віддається саме інформаційній безпеці держави. Країни ЄС, в свою чергу, демонструють більш послідовну політику щодо гарантування і дотримання прав і свобод людини в інформаційній сфері. Про це свідчать, зокрема, останні зміни в законодавстві щодо захисту персональних даних. Окрім того, значну роль у нормотворчості відграють міжнародні судові органи, зокрема суд ЄС та ЄСПЛ, які шляхом правозастосування конкретизують розуміння змісту правових норм на основі суспільної практики, а часом і формують нове розуміння з огляду на зміни, що відбуваються в суспільстві. Натомість, Радзієвська О.Г. зазначає, що норми міжнародного права і законодавства ЄС, а також досвід іноземних держав свідчить про існування двох моделей забезпечення інформаційної безпеки: людиноцентричну (країни Європейського Союзу, США) та державоцентричну (РФ, КНР) [225]. Частково не поділяємо поглядів автора щодо моделі забезпечення інформаційної безпеки США, адже хоча безперечно, США закріплено конституційно принцип пріоритету прав, свобод і законних інтересів людини і громадянина. Проте, аналіз законодавства США у сфері інформаційної безпеки свідчить про пріоритетність окремих напрямів забезпечення національної кібербезпеки США, зокрема, захист критично важливих об’єктів інфраструктури. При визначенні принципів правового регулювання відносин, що виникають з приводу інформаційної безпеки людини, вважаємо, що вони мають базуватись на основних засадах (1) правового регулювання інформаційної сфери; (2) правового 362 регулювання у сфері інформаційної безпеки та (3) правового регулювання прав і свобод

людини. Таким чином, до основних принципів правового регулювання відносин у сфері інформаційної безпеки людини пропонується віднести: - принцип пріоритету прав, свобод і законних інтересів людини і громадянина; - принцип свободи інформації і обмеження доступу до інформації виключно у випадках передбачених законом; - принцип розвитку сприятливого для людини інформаційного суспільства; - принцип відповідальності держави перед людиною та суспільством за реалізацію державної політики інформаційної безпеки; - принцип мінімізації негативного інформаційного впливу на людину, в т.ч. шляхом формування інформаційної культури людини і суспільства; - принцип участі громадянського суспільства у розробці та контролю за реалізацією заходів щодо попередження та захисту від загроз інформаційній безпеці людини; - принцип гармонізація інформаційного законодавства України із законодавством ЄС та положеннями міжнародного права у сфері інформаційної безпеки. Базуючись на запропонованих принципах, механізм правового регулювання має включати систему правових засобів, організованих найбільш послідовним чином з метою попередження, нейтралізації, обмеження та подолання загроз інформаційній безпеці людині. В теорії права відсутнє єдине бачення визначення елементів механізму правового регулювання. Скакун О.Ф., як елементи механізму правового регулювання визначає:

1) ті, що діють на відповідних стадіях регулювання - норми права; нормативно-правові акти; юридичні факти; правовідносини; акти безпосередньої реалізації суб'єктивних юридичних прав і обов'язків;

2) ті, що діють протягом усього регулювання - суб'єкти, що здійснюють правове регулювання чи правову діяльність; правова законність, правосвідомість, правова культура,

3) ті, що мають факультативний характер - інтерпретаційно-правові 363 акти, акти застосування норм права [115].

Онищенко і Зайчук вважають, що сучасна юридична наука характеризується наявністю двох підходів до визначення елементів механізму правового регулювання[123]. Перший, широкий підхід, передбачає наявність

сукупності елементів, які беруть участь у процесі впорядкування суспільних відносин, а саме: норми права,; нормативноправового акту; юридичних фактів; правовідносин; тлумачення і реалізація права; законність; правосвідомість і правову культуру; правову поведінка та юридична відповідальність. Досліджуючи проблеми правового регулювання у сфері інформаційної безпеки людини під таким кутом, поруч з категорією правова культура необхідно звернути увагу на інформаційну культуру, яка втілюється в культурі формування інформаційних потреб, впровадження і використання інформаційних технологій, удосконалення інформаційної діяльності, відповідних правовідносин тощо і є чинником інформаційної цивілізації. Бєляков К.І., Шопіна І.М. і Онопрієнко С.Г., досліджуючи феномен інформаційної культури, зазначають, що істотні інформаційно-глобалістичні перетворення в соціумі зумовлюють постійний розвиток і видозміну форм суспільної комунікації, виникнення новітніх суспільних відносин, що не може не позначитися на правовій системі, а отже, на правосвідомості і правовій культурі, правовому вимірі в цілому [45]. Вони визначають перелік основних нових загроз, зокрема правового характеру, подолання яких є одним із пріоритетів держави і суспільства на шляху подальшого розвитку.

По-перше, це нові деформації правосвідомості. Уявний "віртуальний світ" негативно впливає, передусім, на молодь, свідомість якої перебуває на стадії формування, зменшуючи потреби і здатності людини в реальних соціальних контактах. Це негативно позначається на правовій активності та викликає проблеми соціалізації.

По-друге, швидкість розвитку інформаційних відносин значно перевищують темпи правового розвитку, що зумовлює певне відставання наявних правових механізмів від реальних соціальних потреб у правовому впорядкуванні інформаційної сфери.

По-третє, інформаційні технології стали новим простором і знаряддям для вчинення правопорушень. Зокрема, як приклад, вони наводять саме технології негативного інформаційного впливу на свідомість людини.

Швидкість, анонімність, латентність, транскордонність таких правопорушень вимагають суттєвого удосконалення національного законодавства, діяльності судової і правоохоронної систем, а також запровадження додаткових напрямів освіти, спеціальної підготовки і перепідготовки представників юридичної професії з метою формування відповідного рівня інформаційної культури.

По-четверте, глобалізація розмиває соціокультурні межі суспільств різних країн. Відбувається інтеграція правових систем, вироблення універсальних правових форм і процедур, глобальних важелів управління. Надмірна уніфікація правового життя світового суспільства може спричинити втрату ідентичності національних правових систем, інформаційного суверенітету та їхнього культурного розмаїття, що також є глобальною загрозою [45].

Не відкидаючи цінність широкого підходу, який дозволяє розглядати механізм правового регулювання в єдності з важливими елементами правової дійсності – правовою культурою та правосвідомістю, все ж автор більш схильний до другого, вузького, підходу, який включає лише елементи, які складають основу регулятивної функції права, наприклад в [142]. Серед них виділяють: норми права і принципи права, об'єктивовані в законах та підзаконних нормативноправових актах, акти тлумачення права (інтерпретаційні акти), акти застосування норм права (правозастосовчі акти), правовідносини, суб'єктивні права та юридичні обов'язки суб'єктів правовідносин. Кожен з елементів даної системи виконує специфічну функцію у задоволенні інтересів суб'єктів, в регулюванні суспільних відносин, у досягненні ефективності правового регулювання.

Норма права є основою механізму правового регулювання. Вона встановлює можливий варіант поведінки (активної чи пасивної), визначає суб'єктивні права та можливості реалізувати охоронюваний законом інтерес, так і необхідний варіант поведінки – юридичні обов'язки. Завдання норми права в механізмі правового регулювання полягає в тому, щоб: а) визначити загальне коло учасників правовідносин (взагалі, у конкретних правовідносинах зокрема);

б) встановити зміст суспільних відносин (зміст поведінки суб'єкта), а також об'єкти правовідносин; в) визначити гіпотезу чи обставини, за яких слід керуватися даним 365 правилом поведінки; г) розкрити саме правило поведінки (диспозиція) вказівкою на права і обов'язки (зміст) учасників відносин, що регулюються, характер їх зв'язку між собою, а також державно-примусові заході, що можуть бути застосовані при невиконанні юридичних обов'язків [300]. Якість правового регулювання значною мірою залежить від того, наскільки норми права враховують закономірності суспільних відносин, що регулюються, а також від рівня правової культури як законотворців зокрема, так і суспільства в цілому. Тому, правове регулювання відносин. що виникають з зв’язку інформаційною безпекою людини є можливим і ефективним лише у випадку розуміння як першими, так і другими інформаційної безпеки людини як необхідної умови її існування і розвитку в інформаційному суспільстві. Нормам інформаційного права властиві як загальні ознаки - державно-владна природа, загальнообов’язковість, формальна визначеність і структурованість, так і специфічні ознаки, обумовлені насамперед комплексним характером цієї галузі законодавства. До таких специфічних ознак Ковленко Л.П. віднесла: вираження державного інтересу; переважно імперативний характер, їх реалізація підкріплюється можливістю застосування засобів державного примусу; є регулятором інформаційних відносин; пов’язані з реалізацією інформаційних прав і свобод; наявність специфічних способів реалізації інформаційних норм [198]. Слід зазначити, що норми інформаційного права на сьогодні є розпорошені в великій кількості нормативних актів, що суттєво знижує ефективність правового регулювання всієї інформаційної сфери.

Тому підтримуємо позицію багатьох вчених (Бєлякова К.І., Баранова О.А., Цимбалюка К.І., Пилипчука В.Г. та інших), які вже понад 10 років звертають увагу на необхідність систематизації норм у цій сфері шляхом прийняття Інформаційного кодексу. Так, абсолютно переконливою вважаємо позицію Баранова О.А., що систематизація норм інформаційного права повинна забезпечити: створення єдиної і несуперечливої системи класифікації норм і

нормативно-правових актів; стабілізацію інформаційного законодавства; внутрішню єдність інформаційного права та інформаційного законодавства за рахунок групування правових норм згідно з прийнятим алгоритмом; аналіз поточного стану інформаційного законодавства та усунення наявних прогалин і суперечностей; виключення дублюючих правових норм; єдине використання основних термінів; ефективність пошуку необхідних правових норм; підвищення ефективності правотворчої та правозастосовної діяльності у галузі інформаційного права тощо [24]. Також підгримуємо позицію вченого, що офіційна структура інформаційного законодавства в державі не відповідає структурі інформаційного права, що є однією із причин його нерозвиненості та недосконалості, а також відставання від вимог сучасності в частині розвитку інформаційного суспільства [24].

Окрім того, така невідповідність негативно впливає на нормотворчу та правозастосовну діяльність, оскільки аналіз і тлумачення несистемних і часто суперечливих норм вимагає глибокого розуміння правової природи інформаційних відносин, що не завжди має місце на практиці. Нормативно-правові акти обслуговують нормативну основу механізму правового регулювання. До нормативно-правових актів (законів, підзаконних актів) приєднуються акти, в яких дається їх офіційне роз'яснення, тлумачення. Вони не містять нових правових положень, лише є засобом, який забезпечує однакове розуміння і застосування чинних нормативних актів. Чіткість і ефективність механізму правового регулювання залежать від правильного тлумачення норм права. В Україні основним видом інтерпретаційних актів є акти Конституційного Суду України. А.О. Селіванов та А.А. Стрижак зазначають, що Конституційний Суд України дає офіційне тлумачення Конституції України і порівнюваних з нею законів, інших нормативних правових актів, їх окремих положень, що містить певну нормативність; Конституційний Суд України визначає їх відповідність або невідповідність Основному Закону країни, що є спірним стосовно їх нормативності; рішення Конституційного Суду України є підставою для приведення актів (норм) законодавства (у тому числі трудового)

у відповідність з Конституцією України для вдосконалення права [113]. Так, суттєвої критики зі сторони правозахисників зазнало Рішення Конституційного Суду від 20.01.2012 щодо офіційного тлумачення конфіденційної інформації, коли Конституційний Суд України встановив, що збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди є втручанням в особисте життя і допускається винятково у випадках, визначених законом, і тільки в інтересах національної безпеки, економічного добробуту і прав людини. Хоча досі Конституційний Суд послідовно демонстрував позицію захисту особистого життя людини, але прийняття такого рішення було спрямовано на захист вищих посадових осіб, а не пересічних громадян.

Тим не менш, діяльність Конституційного Суду України, його рішення забезпечують вищу юридичну силу Конституції України, зміцнюють правопорядок і законність у країні, що визначає нормативність для правозастосування; рішення Конституційного Суду України належать до сфери конституційного права; водночас його висновки про оцінку конституційності актів (норм) законодавства, правові позиції, що стосуються регулювання суспільних відносин, тісно пов'язані з правом; вони не належать до нього безпосередньо, є джерелом удосконалення і розвитку галузей права [212]. Важливо, що згідно ст. 46 Конвенції про захист прав людини і основоположних свобод та ст. 2 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» передбачено обов'язковість виконання рішень Європейського суду з прав людини, що на жаль не робить їх джерелами законодавства, як в більшості європейських держав, де вони є актами прямої дії.

Таким чином, на законодавчому рівні закріплено статус рішень Європейського суду з прав людини як джерела права, але керуватись цими рішеннями при розгляді справ чи ні, вирішують саме національні суди. І, на жаль, аналіз правозастосування і постійне зростання кількості звернень від громадян України, що були задовільнені ЄСПЛ, свідчать про небажання керуватися судовою практикою Європейського суду при розгляді справ і, як

наслідок, запобігати подальшим аналогічним порушенням на стадії використання національних засобів правового захисту прав людини. Наступним необхідним елементом механізму правового регулювання є правовідносини, які індивідуалізують положення відповідної правової норми, конкретизують суб'єктивні юридичні права і обов'язки певних суб'єктів, їх повноваження і юридичну відповідальність.

Питання інформаційних правовідносин досліджувались в працях Баранова О.А., Бєлєвцевої В.В., Бєлякова К.І., Брижка В.М., Кормича Б.А., Кохановської О.В., Маріц Д.О., Марущака А.І., Коваленко Л.П., Цимбалюка В.С., та інших. Проте, незважаючи на значний науковий інтерес, відсутній єдиний загальноприйнятий підхід до їх природи і структури. В інформаційній концепції права мається на увазі інформаційна складова будь-яких правовідносин. Проте, переважна більшість науковців визначають інформаційні правовідносини відштовхуючись від права на інформацію, тобто процесів створення, поширення, зберігання, використання та знищення інформації. Особливості прав, обов'язків, повноважень і відповідальності значною мірою обумовлені від регулюючого впливу норм права, у результаті якого складаються різні види правовідносин. Отже, правовідносини в механізмі правового регулювання утворюють певну систему і таким чином забезпечують переведення загальних розпоряджень норм права в суб'єктивні юридичні права і суб'єктивні юридичні обов'язки, повноваження і юридичну відповідальність для конкретних осіб, дозволяють досягти виконання їх волі, задоволення інтересів. Особливої уваги, на нашу думку, заслуговує позиція Баранова О.А., який описуючи інформаційні відносини, звертає увагу на їх зв'язок із: «особливостями життєвого циклу існування (функціонування) суб'єктів інформаційної інфраструктури як юридичних осіб; наданням інформаційних послуг і виконанням інформаційних робіт у процесі створення, поширення (передачі), зберігання, використання та знищення (утилізації) інформації; виробництвом і використанням інформаційних технологій і ресурсів, зокрема із використанням обмежених ресурсів; забезпеченням інформаційної безпеки»

[24]. На основі ґрунтовного аналізу вчений дає наступне визначення інформаційних правовідносин - «суспільні відносини, що регулюються нормами інформаційного права і виникають у процесі обороту інформації, тобто в процесі її створення, поширення (передачі), зберігання, використання та знищення (утилізації), а також у процесі забезпечення обороту інформації між суб'єктами, які мають суб'єктивні права та юридичні обов'язки, що реалізуються методами правого регулювання приватного і публічного права». В механізмі правового регулювання правовідносини виконують наступні функції: окреслюють коло осіб, на яких поширюється дія норми права; закріплюють можливу або необхідну поведінку учасників правовідносин; обумовлюють можливість реалізації спеціальних юридичних засобів з метою забезпечення суб'єктивних прав, обов'язків, відповідальності. Основу правовідносин становить правосуб'єктність, яка складається з правоздатності та дієздатності. Як нами вже зазначалось, формування інформаційного суспільства обумовило не лише значення існуючих і появу нових інформаційних прав людини, а й змінило змістовне наповнення усіх прав і свобод людини, а також її обов’язків, в напрямку формування інформаційної складової кожного з них. Таким чином, актуалізація інформаційних правовідносин обумовлює формування інформаційної правосуб’єктності людини та інформаційно-правового статусу як нового галузевого правового статусу людини. 370 Наступним важливим елементом механізму правового регулювання є акти безпосередньої реалізації прав і обов'язків, які можуть відбуватись в два способи: активний - вчинення дій, що дозволяються (наприклад, використання права на доступ до публічної інформації); пасивний - утримування від заборонених дій (наприклад, нерозголошення інформації з обмеженим доступом). Використання правових норм передбачає реалізацію прав і свобод шляхом виконання активних дій. І в умовах становлення інформаційного суспільства актуалізації великої кількості інформаційних загроз саме використання інформаційних правових норм є бажаною поведінкою суб’єктів інформаційної безпеки. Адже стрімкий і багатовекторний розвиток інформаційного середовища відбувається значно

швидшими темпами ніж розвиток інформаційного законодавства, отже встановлення обов’язкової моделі поведінки. В той же час, свідома і проактивна позиція людини, що базується на використанні наданих законом можливостей дозволяє їй самостійно уникати небезпек. Реалізація обов’язків активними діями свідчить про виконання правових норм. Насамперед, це є очікувана поведінка від органів публічної влади. Адже саме вони уповноважені розробляти та реалізовувати заходи щодо попередження, нейтралізації та усунення реальних та потенційних загроз інформаційній безпеці людини. Утримуванні від вчинення дій, що забороні, свідчить про додержання норм права. Тобто, норми, що встановлюють адміністративну чи кримінальну відповідальність за розголошення інформації з обмеженим доступом, наприклад, реалізуються тоді, коли особа не вчиняє протиправних дій. Отже, акти безпосередньої реалізації у формах використання наданих нормами права можливостей, виконання зобов'язуючого правового розпорядження, додержання правових заборон фактично є кінцевою метою механізму правового регулювання. У процесі правового регулювання стадія застосування норм права є факультативною і полягає у виданні державно-владного акта. Якщо суб'єкти права не є спроможні самостійно реалізувати суб'єктивні права і юридичні обов'язки, держава в особі компетентних органів здійснює застосування норм права (наприклад, блокування доступу до інформаційних ресурсів, винесення обов’язкових приписів, здійснення правосуддя). Акти застосування норм права мають форму рішень, розпоряджень, наказів, вироків тощо. У них персоніфікуються загальні права і обов'язки, а також, за необхідністю, індивідуалізуються санкції. Специфікою акта застосування норм права є можливість його примусового виконання. Акти застосування норм права у механізмі правового регулювання використовуються в таких випадках: коли самі норми права передбачають, що індивідуалізація прав і обов'язків здійснюється органами держави, посадовими особами, а не учасниками відноси; коли суб'єкти відносин, що регулюються, поводяться протиправно: порушують права, не виконують обов'язки.

У цьому разі актом застосування норм права індивідуалізується юридична відповідальність, передбачена нормами права за їх порушення, тобто встановлюється персональна відповідальність правопорушників. У досліджуваній сфері здебільшого має місце другий випадок. Розглянемо, наприклад, акти застосування, що видає Уповноважений Верховної Ради з прав людини у випадках порушення інформаційних прав людини. Свою щорічну доповідь про стан дотримання прав людини та основоположних свобод у 2016 р. відкривали 3 теми, які є визначальними при реалізації європейського вектора розвитку країни, – доступ до публічної інформації, захист персональних даних, боротьба з усіма формами дискримінації. З дня набрання чинності Закону України «Про доступ до публічної інформації» Уповноважений з прав людини здійснює парламентський контроль за дотриманням права людини на доступ до інформації. державним органом контролю за додержанням права на доступ до інформації. Так, 26.10.2014 р., тобто з дати набрання чинності окремими положеннями Закону України «Про прокуратуру» від 14.10.2014 р., уповноваженим особам Секретаріату Уповноваженого Верховної Ради України з прав людини були передані повноваження щодо складання протоколів про адміністративні правопорушення, зокрема, за порушення Закону № 2939 (ст. 212-3 Кодексу України про адміністративні правопорушення. З прийняттям вказаного Закону України «Про 372 прокуратуру» до сфери повноважень працівників Секретаріату було передано не тільки складення протоколів про адміністративне правопорушення у сфері доступу до публічної інформації. Відповідно до п. 8-1 ст. 255 КУпАП уповноважені особи Секретаріату Уповноваженого з прав людини набули повноважень складати протоколи щодо адміністративних правопорушень, передбачених статтею 212-3 (крім порушень права на інформацію відповідно до Закону України «Про адвокатуру та адвокатську діяльність»).

Станом на 26.10.2014 р. стаття 212-3 КУпАП, крім порушень права на інформацію відповідно до Закону України «Про адвокатуру та адвокатську діяльність», передбачала такі правопорушення: неоприлюднення інформації,

обов’язкове оприлюднення якої передбачено законами України «Про доступ до публічної інформації» та «Про засади запобігання і протидії корупції»; порушення Закону України «Про доступ до публічної інформації», а саме: необґрунтоване віднесення інформації до інформації з обмеженим доступом, ненадання відповіді на запит на інформацію, ненадання інформації, неправомірна відмова в наданні інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації; обмеження доступу до інформації або віднесення інформації до інформації з обмеженим доступом, якщо це прямо заборонено законом; ненадання доступу до судового рішення або матеріалів справи за заявою особи, а також інше порушення «Про доступ до публічної інформації»; незаконна відмова у прийнятті та розгляді звернення, інше порушення «Про звернення громадян»; повторне протягом р. вчинення будь-якого з порушень, передбачених чч. 1-6 цієї статті, за яке особу вже було піддано адміністративному стягненню [320]. Протягом 2015 р. перелік адміністративних правопорушень, які передбачені цією статтею та за якими складають адміністративні протоколи виключно уповноважені працівники Секретаріату Уповноваженого з прав людини, значно розширено. Відтак, повноваження було збільшено щодо нових трьох видів адміністративних правопорушень: неоприлюднення інформації, обов’язкове оприлюднення якої передбачено Законами України «Про особливості доступу до інформації у сферах постачання електричної енергії, природного газу, теплопостачання, централізованого постачання гарячої води, централізованого питного 373 водопостачання та водовідведення"; "Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 рр.", "Про відкритість використання публічних коштів"; "Про відкритість використання публічних коштів". А також сім нових адміністративних правопорушень у сфері порушення вимог Закону України "Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 рр.": необґрунтоване віднесення інформації до інформації з обмеженим доступом; ненадання відповіді на запит на інформацію; ненадання інформації, неправомірна відмова

у наданні інформації; неповне надання інформації; неповідомлення про подовження строку розгляду запиту; відстрочення розгляду запиту, крім випадків, визначених законом [320]. Таке передання повноважень мало на меті підсилити ефективність парламентського контролю за дотриманням права на доступ до публічної інформації, забезпечення належної практики застосування Закону № 2939 та запобігання порушенням у цій сфері. Однак його без забезпечення належного ресурсу для виконання цих функцій, реалізація покладених повноважень не є можливою. Подібною є ситуація у сфері захисту персональних даних, контрольні функції щодо яких було передано у тому ж 2014 р. Уповноваженому Верховної Ради України з прав людини. При цьому поклавши функції, чинним законодавством не передбачено достатній обсяг повноважень для їх виконання. Завершення правового регулювання відбувається через безпосередню або опосередковану реалізацію прав і обов'язків учасниками правовідносин. Таким чином, положення юридичних норм втілюються у фактичній реальній поведінці учасників суспільних відносин, на які було спрямовано правове регулювання. Ще одним важливим елементом механізму правового регулювання є метод. У теорії правового регулювання прийнято виділяти два методи правового впливу: • метод децентралізованого регулювання, побудований на координації цілей і інтересів у суспільних відносинах і який застосовується у сфері галузей приватноправового характеру; метод централізованого, імперативного регулювання, що базується на відносинах субординації між учасниками суспільних відносин і що використовується у публічно - правових галузях. Метод інформаційного права, як нової комплексної галузі права, є питанням, що інтенсивно досліджується.

Аналізуючи методи інформаційного права, Баранов О.А. слушно зауважує, що сучасні процеси розвитку суспільства в Україні призводять до того, що зміст конкретних суспільних відносин, які вимагають правового врегулювання, та правосвідомість можуть змінюватися, а в деяких аспектах навіть кардинально. З цього випливає дуже важливий висновок – методи

конкретної галузі права, особливо такого, що зароджується, зокрема інформаційного права, знаходяться в діалектичному розвитку, тому можуть змінюватися як за складом, так за змістом. З врахуванням цього процес дослідження проблематики методів інформаційного права повинен носити постійний характер [29].

В той же час, автори першого в Україні підручника з інформаційного права в 2004 р. визначали, що провідним методом інформаційного права метод комплексного застосування методів конституційного, адміністративного, цивільного, трудового та кримінального права [24]. Коваленко Л.П. під методом інформаційного права пропонувала розуміти сукупність зафіксованих у нормах цієї галузі прийомів (засобів) впливу на суспільні відносини, що складають її предмет, застосування яких дозволяє створити належні умови для реалізації і захисту прав громадян,в інформаційній сфері нормального функціонування інформаційного суспільства [198]. Правове регулювання відносин у сфері інформаційна безпеки здійснювалось переважно імперативними публічно-правовими методами. Проте, розвиток інформаційної сфери і набуття інформацією ознак товару у вигляді інформаційного продукту, з однієї сторони, а також становлення інформаційних прав людини і їх реалізація як особистих немайнових прав людини, з іншої, обумовили також використання цивільно-правового методу.

Окрім того, єдиний правовий механізм державного регулювання згідно стадіям правового регулювання підрозділяється на три компоненти: механізм правотворчості, механізм реалізації норм права і механізм державного примусу. Кожен механізм діє на своїй стадії державного регулювання - правотворчості, правореалізації і застосуванні юридичної відповідальності – і характеризується специфічними, тільки йому властивими правовими засобами. Кожен спосіб державного регулювання реалізуються через суб'єктивні права. Суб'єктивне право утворює зміст дозволеного. При зобов’язувані та забороні – іншим особам передається право вимоги, що спрямовано на виконання активного або пасивного юридичного обов'язку. З цим, насамперед, пов’язана

проблематичність закріплення права людини на безпечне інформаційне середовище. Адже його реалізація буде реальною лише за наявності обов'язків в інших суб’єктів задовольняти потреби, що виникли у цьому зв'язку в уповноваженого суб’єкта. А визначення таких кореспондуючих обов’язків і коло суб’єктів, що взаємодіють в інформаційному середовищі в умовах глобалізації, вбачається неможливим. Отже, розуміння правового механізму державного регулювання суспільних відносин, що виникають у зв’язку з інформаційною безпекою людини, дозволяє: узагальнити явища правової дійсності, що спрямовані на досягнення мети державного регулювання – правопорядку і законності; виявити специфічні функції, що виконують юридичні явища в правовій системі, показати їхній зв'язок між собою і взаємодію; визначити ефективність їх взаємодії, виявити прогалини та окреслити можливі шляхи їх усунення. Правовий механізм державного регулювання є динамічною частиною правової системи суспільства, оскільки його результативність обумовлена ефективністю взаємодії всіх компонентів. Але вивчення його структури на рівні складових не є неповним. Тому, щоб оцінити спроможність правового механізму державного регулювання варто розглядати його компоненти у взаємозв'язку і взаємодії. Проте, це вимагає більш ґрунтовного дослідження, тому визначається нами як перспективний напрямок досліджень.

3.3. Напрями вдосконалення механізмів державного регулювання інформаційної безпеки України

Вироблення правових основ інформаційної безпеки людини вимагає переосмислення підходів до низки напрямів державного регулювання і державної політики. Зокрема, в умовах інтернаціоналізації всіх сфер суспільного життя розвиток законодавства не може відбуватись без врахування глобалізаційних процесів. При цьому, законотворчі органи окремих держав вимушені враховувати стандарти міжнародного права, а також тенденції до

зближення правових систем. Як правило, такі інтеграційні процеси обумовлені геополітичним становищем держави, економічними чинниками, історичними передумовами, а також національною правовою культурою і традиціями державотворення. Гармонізація і уніфікація відбувається за двома напрямками.

По перше, шляхом творення міжнародних актів, укладання міждержавних договорів, а також нормотворчої діяльності міжнародних організацій, які визначають пріоритети, орієнтири, а часом і рамки для розвитку національного законодавства у визначених сферах.

Другий напрям стосується національного нормотворення, коли держави самостійно сприймають і закріплюють в національному законодавстві досвід державного регулювання інших держав чи міжнародноправові тенденції. Інформаційна безпека, як сфера правового механізму державного регулювання, апріорі не може розвиватись без врахування міжнародного правового поля та досвіду зарубіжних країн. Це обумовлено самою істотою інформаційної сфери, яку складно обмежити національними кордонами в демократичній державі. При цьому важливо, що державне регулювання має відповідати не лише обраному політичному курсу, а й базуватись на існуючій суспільній практиці, відповідати нагальним інтересам громадян і запитам суспільства.

Становлення правового забезпечення інформаційної безпеки людини відбувається в конкретних історичних умовах та невіддільне від правового статусу людини в державі, ступеня розвитку демократичних процесів та правової культури суспільства. Інформаційна безпека в системі міжнародної безпеки пройшла різні етапи становлення. В другій половині XX сторіччя міжнародні домовленості здебільшого стосувались забезпечення існування та розвиток інформаційного середовища бізнесу. На межі тисячоліть відбулися значні трансформаційні процеси в геополітиці і внаслідок подвійної трансгранично-національної природи кіберпростору [128] національна політика держав щодо іноформаційної безпеки стає значимою у вимірі зовнішньої політики, оскільки пов’язана з розбудовою інфраструктури. Дубов Д.В. наводить як приклад, що цілком внутрішні питання освітньої сфери (наприклад,

щодо підготовки фахівців ІТсфери) робить це питання частиною зовнішньої політики держави [29]. Тим більше значимим в міжнародному аспекті є правове забезпечення інформаційного простору держави, інформаційних прав і свобод людини, режимів доступу до інформації, зокрема в глобальній мережі, гарантування принципу міжнародного нейтралітету, електронної демократії та інші. І, очевидним є, що опрацювання міжнародних домовленостей у сфері інформаційної безпеки в цілому, і людини зокрема, значною мірою залежить від політичної волі держав, які мають та/чи змагаються за визначальний геополітичний вплив. На сьогодні, до таких держав, насамперед, належать США, Російська Федерація, КНР та ЄС.

На сьогодні у світі сформувалось два основних підходи щодо змісту міжнародної інформаційної безпеки. Перша група країн демонструє підхід до проблематики міжнародної інформаційної безпеки в широкому розумінні , в основу якої мають бути покладені принципи неподільності безпеки та відповідальності держав за свій інформаційний простір.

Друга група країн звужує питання міжнародної інформаційної безпеки до міжнародної кібербезпеки і такий підхід зосереджується на боротьбі із злочинами у сфері інформаційнокомунікаційних технологій, в т.ч. боротьбу із кібертероризмом. Як наслідок, при цих підходах простежується різне розуміння місця інформаційної безпеки людини в складній системі інформаційної безпеки як на міжнародному, так і на національному рівнях.

Перший підхід, на нашу думку, передбачає узаконення значного простору для обмеження інформаційних прав і свобод людини на користь гарантування інформаційного безпеки міжнародної спільноти і окремих держав. При цьому, прихильниками такого розвитку міжнародної політики виступають здебільшого держави, що мають значні проблеми щодо реалізації конституційних засад демократії, або ж взагалі не визнають демократичних цінностей.

Другий підхід визначається значно більшим соціальним і економічним спрямуванням, передбачає встановлення міжнародних стандартів для

інформаційних прав та свобод людини (особливо пов’язаних з використанням мережі) на достатньо високому рівні. При цьому не передбачає втручання в питання інформаційного суверенітету, ведення інформаційних воєн та деякі інші аспекти політичної і військової сфери. Безперечною вбачається цінність напрацювання міжнародних стандартів як орієнтирів для підвищення рівня захисту прав і свобод людини в інформаційній сфері. Водночас, як свідчить аналіз становлення інституту прав людини у складі міжнародного права, їх значення здебільшого є прогностичним і полягає у виконані таких функцій як: визначають перелік прав та свобод, які відносяться до категорії основних та обов’язкових для всіх держав-учасниць відповідних міжнародних угод або конвенцій; формулюють головні риси змісту прав та свобод, які повинні втілюватись у відповідних конституційних та інших нормативних положеннях окремих держав; встановлюють зобов’язання держав щодо визнання та забезпечення проголошених прав та свобод, а також встановлення на міжнародному рівні гарантій, необхідних для реалізації і захист. прав та свобод; фіксують умови щодо застосування прав та свобод людини, одночасно із законними обмеженнями цих прав та свобод [256].

Проте, інформація та інформаційні технології у сучасному світі є одночасно і основним ресурсом, поруч з енергією і матерією, водночас є джерелом загроз, що вимагає інших підходів до етичної оцінки та державного регулювання питань, пов'язаних з технологіями. Тому стандарти прав і свобод людини в інформаційному суспільстві визначається не лише особливостями національного співтовариства людей, а й розвитком людської цивілізації в цілому, рівнем інтегрованості міжнародного співтовариства, а також з огляду на реальні та потенційні загрози інформаційній безпеці. Для прикладу, 1 жовтня 2017 р. набув чинності Закон про захист мереж, який раніше називався "Законом про Facebook", нормами якого передбачено обов’язок соціально-медійних компаній в Німеччині вилучати підроблені новини або повідомлення, що містять мову ненависті протягом 24 годин.

Насамперед, це стосуватиметься Facebook, Twitter, YouTube та інших сайтів з більш ніж 2 мільйонами користувачів у Німеччині. Покарання застосовуватимуться лише у межах Німеччини, але міністр юстиції Німеччини Хайко Маас, ініціатор закону, заявив, що буде наполягати на подібних заходах у всьому Європейському Союзі [84]. Подібні ініціативи вже довший час обговорюються в ЄС, і зустрічають як підтримку, з огляду на значну кількість дипломатичних, викликаних фейковими новинами, так і критику захисників вільного мовлення. В Україні відсутнє ефективне державне регулювання питань як щодо мови ворожнечі (ненависті), так і з питань дезінформації. При цьому, в умовах постійного інформаційного противоборства, вважаємо, що це одне з першочергових питань, що мало би вирішуватись як на рівні законодавства, так і шляхом відповідних організаційних заходів, які б дозволили не лише зменшити деструктивний вплив дезінформації і мови ненависті на населення, а й відновити порушені права осіб чи навіть соціальних груп. Важливо зауважити, що рішення ЕСПЛ на сьогодні не визнаються в Україні джерелами законодавства, що не виключає можливість їх використання як джерел права. Отже, на нашу думку, врахування аналізу практики ЄСПЛ щодо справ, для вдосконалення національного законодавства в напрямку зближення до міжнародних стандартів, а також усунунення недоліків національного законодавства, які спричинили порушення, що стали предметом розгляду.

Як свідчить досвід країн з розвиненою демократією, інформаційна безпека людини не повинна протиставлятись інформаційній безпеці держави та суспільства. Адже саме людина визнається основною цінністю кожного суспільства і забезпечення її прав і свобод є кінцевою метою реалізації функцій держави. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держав, попередження міжнародних конфліктів чи/та терористичних актів, а також забезпечення безпеки національних інформаційних ресурсів.

Таким чином, має місце конфлікт інтересів різних об'єктів інформаційної безпеки. Вирішення цього конфлікту демократичним шляхом є однією з первинних задач при створенні відповідних правових норм. Тому, нагальною потребою вбачаємо необхідність розробки і прийняття базового закону для досліджуваної сфери - «Про інформаційну безпеку», в основу якого може бути покладено запропоновані нами в попередньому підрозділі принципи, а також досвід іноземних держав. Як бачимо, підходи США і ЄС до вирішення цього питання суттєво відрізняються. Про це свідчить як аналіз законодавства, так і правозастосування. США декларує високі стандарти прав і свобод людини в інформаційній сфері, але при виникненні протиріч між гарантуванням дотримання цих стандартів і інтересами національної безпеки перевага віддається саме інформаційній безпеці держави. Країни ЄС, в свою чергу, демонструють більш послідовну політику щодо гарантування і дотримання прав і свобод людини в інформаційній сфері. Про це свідчать, зокрема, останні зміни в законодавстві щодо захисту персональних даних. Окрім того, політика ЄС у інформаційній сфері характеризується узгодженістю і забезпечується дієвими механізмами реалізації. Значну роль нормотворчості відграють міжнародні судові органи, зокрема, суд ЄС та ЄСПЛ, які шляхом правозастосування конкретизують розуміння змісту правових норм на основі суспільної практики, а часом і формують нове розуміння з огляду на зміни, що відбуваються в суспільстві. Зокрема, про це свідчить аналіз рішень у справах ЄСПЛ щодо права на доступ до інформації, який відображає зміну розуміння цього права, а також його співвідношення з іншими інформаційними правами, зокрема правом на захист персональних даних, свободою вираження поглядів тощо. Україна, обравши шлях євроінтеграції і підписавши угоду про асоціацію з ЄС взяла на себе зобов'язання щодо адаптації законодавства з відповідними нормами ЄС.

Відповідно, значні зусилля спрямовуються власне на приведення у відповідність вже існуючого законодавства. Проте самих змін в законах не достатньо. Правове регулювання має відображати бажані соціальні зміни і їх

стимулювати. Великим викликом для українського суспільства є нерозуміння доцільності окремих змін в правовому регулюванні інформаційної сфери. Для прикладу, спостерігається брак підтримки з боку державних органів та органів місцевого самоврядування оприлюднення публічної інформації у вигляді відкритих даних. В свідомості багатьох чиновників все ще має місце «радянське» мислення - інформація належить державі, в особі її уповноважених органів. В демократичному ж суспільстві інформація накопичена публічними органами є власністю громадянського суспільства, яке вільне використовувати її на власний розсуд (або не використовувати). Про це також говориться в Рекомендації ЮНЕСКО з використання та розвитку багатомовності та загального доступу до всесвітнього електронного простору, де надане визначення інформації, що є суспільним надбанням: «Інформацією, що є суспільним надбанням, вважається доступна для населення інформація, використання якої не порушує жодних передбачених законом прав або зобов'язань щодо дотримання конфіденційності». Одним з пріоритетів демократичного суспільства є надання права всім членам на доступ до інформації і знань і на їх використання на виконання однієї з основних громадянських свобод - свободи вираження та свободи участі у культурному житті і науковому прогресі. Для досягнення цієї мети державними органами створюється значні обсяги інформації, істотна частина якої має бути відкритою для вільного розповсюдження через інтернет, бібліотеки та інші пункти публічного доступу, а також за допомогою таких інструментів розвитку суспільства, як бізнес і освіта. Оскільки законодавство і політика більшості країн в основному орієнтовані саме на захист інформації, на яку поширюються права власності, роль і значимість інформації, що є суспільним надбанням, особливо інформації, створюваної державними установами, часто недооцінюється.

В Керівних принципах ЮНЕСКО в політиці вдосконалення державної інформації [32], що є суспільним надбанням, метою було визначено сприяння вдосконаленню інформації, що є суспільним надбанням, на урядовому рівні,

причому особлива увага приділена поширенню інформації в електронному форматі. Іноземний та міжнародний досвід свідчить, що створення самого лише правового поля в цій сфері виявляється недостатнім для досягнення мети – демократизації суспільства і забезпечення реалізації інформаційних прав громадян, проте дозволяє розширите можливості для їх використання в інтересах людинки і суспільства Так, у Сполученому Королівстві відкриті дані є не лише відповіддю на суспільний запит, але при ефективному використанні приносять 2- 5% ВВП. В Великобританії понад 70% комерційних організацій користується відкритими даними. При цьому доступні і належним чином викладені відкриті дані є сигналом для потенційних інвесторів.

Держава не спроможна самостійно розбудовувати сервіси на основі цих масивів інформації, якими володіє. Створення належної правової бази означає вирішення таких питань – визначання процедури розкриття даних, яка б не залежала від бажання посадових осіб розпорядників інформації, забезпечення належної форми оприлюднення таких даних, визначення механізмів захисту прав на доступ до таких даних. Закон про доступ публічної інформації містить окремі положення щодо відкритих даних, проте ним не передбачено шляхів забезпечення виконання цих положень і органів, що мали би здійснювати відповідний нагляд. Що стосується відкритих даних, що не належать державі, то їх системне правове регулювання відсутнє. Відсутнє на рівні законодавства і визначення відкритих даних, порядок надання такого статусу і його зміст. На нашу думку, має бути закріплено на нормативно-правовому рівні, що інформація (дані) є відкритою, якщо будь-хто має до нього вільний доступ, може вільно використовувати та ділитися нею. Ще одним важливим кроком у напрямку підвищення стандартів захисту інформаційної безпеки людини вбачається створення інституту на зразок інформаційного комісара – як незалежного органу, діяльність якого спрямована на захист прав і свобод людини в інформаційній сфері. Інституція Інформаційного комісара нині існує в Туреччині, Словаччині, Великобританії, Португалії та Словенії.

Досвід цих країн свідчить, що така незалежна інституція займається питаннями захисту прав громадян, журналістів та громадських активістів у справах з доступу до інформації, а також має набір повноважень щодо забезпечення захисту персональних даних. Створити єдиний орган інформаційного комісара, у компетенції якого була б робота з двома правами: доступ до публічної інформації та захист персональних даних, також рекомендують експерти Ради Європи. Зокрема, голова офісу Ради Європи в Україні М. Енберг назвав її «ключовою рекомендацією Ради Європи щодо аналізу та розподілу повноважень держустанов у сфері інформаційної політики та медіа в Україні» [95]. Суспільна думка та позиції політикуму щодо цього питання суттєво змінились за останні 10 років. В 2008 р. дослідження діяльності омбудсмана по здійсненню контролю за додержанням права на доступ до інформації, дозволяло стверджувати, що – Уповноважений Верховної Ради з прав людини не приділяє належної уваги цій проблемі. Зокрема, висвітлюючи в щорічних доповідях стан забезпечення в Україні інформаційних прав, уповноважений розглядав лише проблеми пов'язані зі свободою інформації та свободою ЗМІ. В доповідях не аналізувалась ситуація щодо забезпечення доступу до інформації в Україні й лише опосередковано згадувалась проблема неправомірного застосування органами виконавчої влади грифів, що не визначені жодним нормативним актом: «для службового користування», «не для друку», «опублікуванню не підлягає». У зв'язку з тим, що кількість звернень на адресу Уповноваженого з прав людини про порушення органами державної влади права громадян на доступ до інформації, становила за рік у середньому від 0,1 до 0,3 відсотка загальної кількості звернень, Уповноважений Верховної Ради з прав людини вважав не актуальним запровадження посади спеціалізованого омбудсмана з питань інформації [275]. Проте, вже в 2017 р. діючий Уповноважений Верховної Ради з прав людини, на якого покладені відповідні повноваження, провадить чітку політику підтримки створення такого незалежного інституту, зокрема на рівні законодавчих ініціатив. Під час міжнародної конференції «Відзначення 250-ї річниці права на

інформацію та подальше зміцнення всіх національних систем країн Східного партнерства», Валерія Лутковська зазначила про необхідність створення інституції Інформаційного комісара: «Ми маємо низку проблемних питань у цьому зв'язку.

По-перше, рекомендації Уповноваженого з прав людини, як і в більшості країнахчленах Ради Європи, не є обов'язковими до виконання, а це в свою чергу, знижує ефективність захисту права на інформацію. По-друге, функція покарання не є притаманною для національної інституції з прав людини. Крім того, функції контролю за доступом до інформації йдуть урозріз з так званими «паризькими принципами» діяльності національної інституції з прав людини» [181]. Нами пропонується впровадження інституції Уповноваженого з інформаційної безпеки людини, для чого є необхідність внесення змін до Конституції України, а також створення правових засад діяльності такого органу, які б надавали достатню кількість інструментів впливу на правопорушників не лише з метою притягнення їх до відповідальності, а й задля відновлення порушеного права, а також запобіганню подальших незаконних обмежено реалізації інформаційних прав і свобод людини. Оскільки не можливо надати вичерпний перелік інформаційних загроз людині, бо вони модифікуються з розвитком інформаційних технологій і самого суспільства, то необхідним вбачається надання відповідних повноважень щодо моніторингу інформаційних загроз людині і суспільству. Прикладом може бути ситуація, що склалася з приводу прийняття Закону «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [348].

Ще до набрання ним чинності точилася публічна дискусія щодо його суперечливого характеру і загрози правам і свободам людини. Зокрема, Українська гельсінська спілка з прав людини ще на етапі законопроекту звертала увагу на надмірно розширений перелік цілей з якими створюється реєстр, а також недоцільність в умовах сучасної України, «збирати таку низку персональних даних про особу в єдиному реєстрі, а з метою більшого

забезпечення права особи на приватність, рекомендовано мати декілька реєстрів, причому з забороною об'єднувати 385 інформацію з різних реєстрів без згоди особи»[440]. Окрім того, Закон не розрізняє загальні і вразливі дані. Критиці з боку правозахисників Закон піддавався і після прийняття [137]. Певна кількість недоліків була усунена, проте все ще залишається відкритими значна кількість питань – які суб'єкти (крім самої фізичної особи, дані якої обробляються, та розпорядника Реєстру), за яких обставин, на якій підставі та за якою процедурою можуть мати доступ до інформації, яка зберігається в Реєстрі, не визначено строків зберігання та обробки інформації в Реєстрі, відсутня процедура знищення персональних даних, необхідність зберігання яких у Реєстрі більше не існує та інші.

Важливим питанням також залишається етичність впровадження єдиного незмінного реєстраційного номеру особи. Українська гельсінська спілка з прав людини ґрунтує заперечення на декількох підставах: «По-перше, заперечення морального характеру. Призначення особі незмінного реєстраційного номеру, який проставлятиметься на всіх документах принижує гідність особи, ототожнює особу з набором цифр, який отримується за допомогою невідомого алгоритму. Більше того, така практика призначення державою номера замість імені характерна для тоталітарних держав, перш за все в концтаборах. Нагадаємо, що під час Нюрнберзького процесу Міжнародний воєнний трибунал визнав практику присвоєння особам знеособлюючих номерів і клейміння осіб ними злочином проти людяності. Можна сказати, що ототожнення особи з певним кодом не лише посягає на право особи на ім'я, але й нав'язує особі відчуття власної незначущості. На жаль, історія існування Української держави свідчить про те, що цій державі громадянин майже ніколи не може беззастережно довіряти, тож невідомо з якою метою буде насправді використано зібрану інформацію. Подруге, як показало впровадження податкового ідентифікаційного коду, для низки громадян поставлення коду у відповідність імені є неприйнятним з релігійних міркувань. По-третє, запровадження єдиного реєстраційного номеру особи становить

фундаментальну загрозу праву особи на приватне життя (на приватність). Це значною мірою пов'язане з відсутністю в Україні ефективної системи захисту персональних даних, а гарантії захисту персональних даних, передбачені цим законопроектом, не можна вважати адекватними, тим більше з огляду на практику контролю приватного життя в СРСР і історичну пам'ять про це державних чиновників. Неприйнятним видається і вимога розміщення реєстраційного номеру на всіх документах Реєстру, до яких віднесено низку галузевих документів: права водія, учнівський квиток тощо. Таке положення створить умови для тотального контролю за особою і, відповідно, до порушення права особи на приватність. Крім того вважаємо за доцільне звузити кількість документів реєстру власне до ідентифікаційних документів»[440]. Питання існування реєстрів і їх взаємодії є взагалі дуже чутливим як зі сторони інформаційної безпеки людини, так і з огляду на права та свободи людини в демократичному суспільстві. Норми, що передбачають існування єдиних та державних реєстрів, а також порядок зберігання, реєстрації та надання інформації персонального характеру не завжди визначаються нормами законів. Закріплення подібних норм на підзаконному рівні суперечить п.1 ст. 92 Конституції, який передбачає, що виключно законами України визначаються "права і свободи людини і громадянина, гарантії цих прав і свобод; основні обов'язки громадянина". А реєстри, що порядок ведення реєстрів в установах, підприємствах і організаціях, взагалі часто не відповідає нормам визначеним законом, а особи, що здійснюють ведення таких реєстрів, уявлення не мають про законодавство щодо персональних даних і поводяться з ними неналежним чином. Це призводить до порушення не лише інформаційних прав і свобод людини, а й може становити загрозу її життю і здоров'ю. Для прикладу, персональні дані, що вносяться до реєстрів в медичних установах, у тому числі інформація про стан здоров'я, належать до так званої «чутливої» інформації, тому мають бути ретельно захищені. Розголошення певних видів такої інформації, наприклад, щодо захворювання на онкологічні, неврологічні захворювання тощо, може призвести до соціальної стигматизації [65].

Величезну загрозу для безпеки фізичних осіб може бути створено у зв'язку з внесенням змін до законодавства щодо трансплантації органів та інших анатомічних матеріалів людини.

В законопроекті 2386(а-1), що був прийнятий в першому читанні 21.04.2016 передбачається створення Єдиної державної інформаційної системи трансплантації, яка буде містити інформацію щодо потенційних донорів. При цьому у законопроекті відсутні гарантії забезпечення конфіденційності такої інформації, не визначений механізм захисту та відповідальні суб'єкти забезпечення. Окрім того, відсутній правовий механізм забезпечення доступу реципієнтів до інформації про наявність донорських органів та інших анатомічних матеріалів людини. В умовах, коли країна знаходиться фактично у стані війни, а окрім того має складну криміногенну ситуацію, розголошення персональних даних особи можуть стати підставою для зазіхань на її життя зловмисниками. Тому питання створення будь-яких реєстрів, що містять чутливу інформацію, мають чітко і однозначно регулюватись на законодавчому рівні і відразу визначати суб'єктів, що відповідальні за забезпечення захисту такої інформації та відповідальність у випадку порушення інформаційних прав людини. В той же час, не слід залишати поза увагою, особливості національного інформаційного простору. В умовах гібридної війни, невід'ємною складовою якої є інформаційна, стоїть нагальна потреба ефективного моніторингу ситуації із дотриманням прав всіх суб'єктів інформаційних правовідносин, а також виявлення системних проблем як на рівні правового забезпечення, так і в правозастосовчій діяльності. Інформаційна війна – це завжди атака інформаційної функції, незалежно від засобів, які застосовуються. При цьому ціллю враження є дуже широке коло суб'єктів – від пересічних громадян, членів окремих суспільних груп – етнічних, релігійних, територіальних тощо, до політичних діячів, посадових осіб, від яких залежить прийняття доленосних рішень для всієї держави. Як вже неодноразово звертали увагу, загрози інформаційній безпеці людини значною мірою узалежнені від геополітики. Аналіз ситуації в країнах Східного

партнерства, зокрема досвід Грузії, Вірменії і Молдови в сфері інформаційної безпеки людини є цінним для України з огляду на: (1) проєвропейську політичну спрямованість, а отже і спроби адаптації до законодавства і стандартів ЄС; (2) геополітичну ситуацію, що пов'язана зі значним впливом (в т.ч. інформаційним) 388 зі сторони Російської Федерації; (3) наявність територій, що не підконтрольні уряду, і використання конфліктів в цілях підривання суверенності державної влади; (4) нестійку політичну і економічну ситуацію в середині держави. На пострадянському просторі сьогодні простежується виокремлення двох груп країн, що різко відрізняються принципами формування політики у інформаційній сфері. Про це свідчать також результати опитування 50 експертів ІКТ, які відображені в дослідженні «Ціна свободи і безпеки. Індекс ІКТзаконодавств Євразії за 2016 р. », виконаному DR Analytica на замовлення Digital.Report [97]. У першій групі опинилися Вірменія, Грузія і Молдова: націленість влади цих країн на збільшення свободи у всіх сферах, а також облік економічного ефекту від вжитих заходів дозволяє проводити збалансовану політику, одночасно приводить до збільшення безпеки. Так, зокрема, в Молдові прийняті в 2016 р. правові акти збільшували як свободу, так і безпеку в усіх сферах. Друга група країн, до якої входять Білорусь, Азербайджан, Росія, Казахстан і Киргизстан, в інформаційній політиці віддає пріоритет інтересам безпеки, переважно - державної. Така політика веде до обмеження свободи інформації для особистості і суспільства. Ці країни також беруть за основу реалізовані в Росії законодавчі ініціативи, зокрема, ті закони, що пов'язані з моральною стороною інтернет-контенту, а також з інформаційною безпекою держави. Проблемним питанням в країнах пострадянського простору залишається боротьба з кіберзлочинністю. Хоча в більшості країн ратифікована Конвенція про кіберзлочинність та прийняті відповідні закони по боротьбі з кіберзлочинністю, реалізація їх положень зачасту є малоефективною, зокрема через те, що влада не вважає кіберзлочинність реальною загрозою, якщо вона не загрожує безпосередньо їх режиму або економічним інтересам. Для країн Східного

партнерства актуальною проблемою залишається домінування Російської Федерації в інформаційному просторі. Російська Федерація довгий час домінувала в культурній, політичній та економічній сферах в Євразії, в тому числі в сфері розвитку ІКТ. Останні роки Грузія, Молдова і Україна докладають багато зусиль, щоб дистанціюватися від Росії, проте інші 389 держави Східного партнерства залишаються під суттєвим впливом її геополітичного впливу. Такий вплив обумовлений цілою низкою чинників – економічними зв'язками, енергетичною залежністю, значною насиченістю мережі російськомовним контентом, а також тим, що російські комунікаційні компанії відіграють помітну роль в країнах регіону.

Держави по різному реагують на цю загрозу. Від повного ігнорування (Білорусь, Казахстан, Азербайджан) до спроб створити чи посилити вплив власних альтернативних ресурсів (Вірменія, Грузія) або заборони окремих ресурсів російського виробництва (Молдова). Україна вже має досвід щодо намагання обмежити доступ до російських інформаційних і комунікаційних ресурсів шляхом зобов'язання провайдерів зробити їх технологічно недоступними. Указ Президента від 15 травня 2017 р. № 133/2017 щодо затвердження рішення Ради національної безпеки і оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 28 квітня 2017 р. викликав бурхливу реакцію громадськості і поставив низку питань щодо його законності, правомірності, допустимості в демократичному суспільстві, а також результативності. Щодо законності цього рішення слід звернутись Конституції України, де ст. 92 встановлює, що «виключно законами України визначаються: права і свободи людини і громадянина, правові засади і гарантії підприємництва, основи національної безпеки…», а ст. 107 - «Рада національної безпеки і оборони України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони». Стаття 10 закону «Про Раду національної безпеки і оборони України» говорить: «Рішення Ради національної безпеки і оборони України, введені в дію указами Президента України, є обов'язковими

до виконання органами виконавчої влади», тобто рішення РНБО не поширюються на приватних осіб і приватні компанії. Укази президента сили закону не мають.

Таким чином, цей акт не може бути визнаний конституційним. Викликають сумніви і правомірність та допустимість в демократичному суспільстві такого рішення. Хоча, Указ президента і рішення Ради національної безпеки і оборони України про введення санкцій за своєю суттю є "адресними", тобто зачіпають тільки юридичних та фізичних осіб, зазначених в цих документах, а також покладають обов'язки щодо реалізації положень рішення на деякі держоргани – Національний банк України, Кабінет міністрів та Службу безпеки України. Проте, фактично цим Указом встановлюється обов’язок провайдерів обмежити доступ до певних ресурсів, що опосередковано визначає неможливість доступу до них окремих громадян. В сучасному суспільстві доступ до інтернету та його ресурсів пов’язаний з реалізацією низки конституційних прав і свобод людини і громадянина, зокрема: прав на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31), недоторканність особистого і сімейного життя (ст. 32), свободу думки і слова, на вільне вираження своїх поглядів і переконань (ст. 34), свободу світогляду і віросповідання (ст. 35), на мирне зібрання (ст. 39), право власності, у тому числі інтелектуальної (ст. 41), на підприємницьку діяльність (ст. 42), на працю (ст. 43), на освіту (ст. 53), на свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв’язку з різними видами інтелектуальної діяльності (ст. 54).[300] Рекомендація Комітету міністрів державам-членам Ради Європи щодо свободи в інтернеті від 13 квітня 2016 р. звертає увагу, що право на доступ до інформації є правом інструментальним, тобто необхідне для реалізації інших прав і свобод людини. А його обмеження має бути необхідним в демократичному суспільстві і пропорційним визначеній законній меті. Наостанок, виникає питання, яку саме мету переслідували творці цього рішення. Якщо ж йшлося про виведення з українського ринку окремих

інформаційних технологій російського виробництва, то ця мета досягнута майже цілком. Проте підприємці змушені були понести додаткові витрати на заміну відповідних технологій, а також у зв'язку з обмеженням доступу до відповідних ресурсів. Викликає обґрунтовані сумніви допустимість такого розв'язання у демократичному суспільстві. Якщо йдеться про обмеження негативного інформаційного впливу на користувачів, то ця мета частково досягнута. Проте залишається можливим використання доступу до заборонених ресурсів через VPN, а також з-за меж України. А суспільний резонанс цього рішення відрізняється від крайнє радикальної підтримки («давно пора було це зробити») до критики як змісту, так і форми реалізації рішення. При цьому, має місце також і нігілістичне ставлення, що виявляється у ігноруванні обмежень і використання технологій для їх обходу і доступу до заборонених ресурсів. Абсолютно логічною в цих умовах є позиція О. Гелетканича: «Інтернет створювався як місце свободи, тому повністю обмежити або заблокувати доступ до ресурсу фактично неможливо через саму природу мережі» [53]. Таким чином, безсистемність і відсутність єдиного концептуального підходу до правових основ інформаційної безпеки людини призвели до появи значних проблем у правозастосовній діяльності. Зокрема, єдиним легальним способом блокування інтернет-ресурсів, що здійснюють незаконну діяльність на сьогодні є судовий. В той же час, протягом останніх років мали місце неодноразові спроби внесення до національного законодавства змін, які б встановлювали нові позасудові механізми блокування інтернет-ресурсів, що суперечить свободі інформації. В той же час, чинне законодавство не визначає порядку витребування інформації (даних) від операторів мереж передачі даних, а також відповідальності за невиконання обов'язку щодо розміщення реальної інформації щодо власників інтернет-ресурсів.

Аналізу правозастосовної діяльності та судової практики свідчить про відсутність належного правового регулювання порядку фіксації об'єктів в інтернеті для пред'явлення їх в суді та інших органах. Забезпечення збору та фіксації доказів в інтернеті є проблемою насамперед, для захисту авторських

прав, але також і у інших випадках – наприклад, передвиборча агітація в день виборів, шахрайство, захист честі, гідності та ділової репутації, втручання в особисте життя тощо. З моменту порушення і до моменту судового розгляду інформація, що розміщена на певній веб-сторінці, може бути неодноразово змінена, більше того така веб-сторінка взагалі може зникнути. Крім того, аналіз норм законодавства, правозастосовної практики та наукових поглядів свідчить про існування кількох способів фіксації змісту вебсторінки.

Таку фіксацію можуть здійснювати особи, чиї права порушуються; треті особи (наприклад, в РФ це нотаріуси); суд або правоохоронні ограни. При цьому така фіксація може бути здійснена як візуальним так технологічним способом. К.О. Зеров пропонує до візуальних способів фіксації слід віднести:

1) Роздруківка веб-сторінки (Web-скріншот);

2) Фіксація особою контенту, що міститься на вебсайті, шляхом його збереження на відповідних носіях (CD, DVD, магнітні диски, тощо);

3) Протокол огляду веб-сторінки нотаріусом;

4) Огляд доказів судом за їх місцезнаходженням;

5) Проведення відеозапису процесу дослідження будь-якою заінтересованою особою;

6) Проведення протоколу огляду веб-сайту адвокатом на підставі його професійного права на збирання відомостей про факти, що можуть бути використані як докази відповідно до п. 7 ч. 1 ст. 20 ЗУ «Про адвокатуру та адвокатську діяльність»; а до технологічних спосіб фіксації (тобто таких, що приділяють увагу технічним аспектам функціонування веб-сторінок) слід віднести: 1) Довідки, отримані від провайдерів (log-файли); 2) Миттєву фіксацію веб-сторінок за допомогою приватних онлайн-сервісів; 3) Використання сервісу InternetArchive. WaybackMachine; 4) Проведення експертного дослідження за експертизою 10.17 – дослідження телекомунікаційних систем (обладнання) та засобів. засобів [92]. Водночас, слід звернути увагу, що візуальні способи фіксації не передбачають аналізу вихідного коду веб-сторінки, що вбачається недостатнім для встановлення

особи правопорушника. Жодний з візуальних способів фіксації змісту веб-сторінок не в змозі дати належне і достовірне уявлення про те, що ж насправді розміщується (і чи розміщується) на даній вебсторінці і чи не була вона модифікована, оскільки такий спосіб є лише відтворенням (останнім етапом використання твору в інтернеті), яке подається на пристрій виведення інформації, а не дослідженням її внутрішньої структури (що здатне довести правомочності відтворення та надання твору до загального відома публіки)[92]. Слід звернути увагу, що жоден з цих способів не має однозначного закріплення в процесуальному законодавстві. Така прогалина законодавства є порушенням конституційного права людини на захист, оскільки в більшості випадків унеможливлює надання доказів, що пов'язані з порушенням інформаційної безпеки та прав людини за допомогою інтернету. Зазначені приклади вказують на системну проблему, що має місце у правовому забезпеченні інформаційної сфері в цілому, і інформаційної безпеки людини зокрема.

Стан українського законодавства у інформаційній сфері свідчить про його невпорядкованість, неузгодженість та безсистемність. Окрім того, слід зазначити, що на сьогодні інформаційна сфера розглядається і як відносно самостійна сфера, і як складова інших видів діяльності. Другий підхід свідчить про те, що інформаційна сфера обслуговує практично всі аспекти суспільного життя – державотворення, безпеку, оборону, економіку, фінансову та грошову системи, соціальну сферу, екологію, науку, освіту і культуру, міжнародне співробітництво. Відповідно, інформаційна безпека виступає і як самостійна сфера регулювання, і, відповідно, є складовою всіх інших – національної, екологічної, економічної, військової та інших. Таким чином, законотворення у сфері інформаційної безпеки не може відбуватись відокремлено від розвитку системи права частиною якого воно є. Розвиток законодавства у цій сфері вимагає ефективної співпраці органів державної влади, інститутів громадянського суспільства, комерційних структур і наукового потенціалу держави. Розробка законодавства щодо інформаційної безпеки людини вимагає створення ефективних механізмів активної участі у законотворчій діяльності її

суб’єктів - належний доступ до проектів нормативних актів у цих сферах, реальні публічні обговорення, а також врахування їх результатів. Цінним в цьому аспекті є досвід держав з напрацьованими інструментами е-демократії – наприклад, Сполученого Королівства, Естонії. Актуальною проблемою залишається необхідність вироблення єдиних техніко-юридичних та мовно-термінологічних вимог до підготовки проектів законів у інформаційній сфері. Оскільки ця сфера відносно нова, надзвичайно динамічна і наукоємна, то й вимагає використання наукового потенціалу при розробці законопроектів у цій сфері, а також проведення експертного оцінювання ефективності вже існуючого законодавства. Цінним з цих позицій вбачається досвід США та окремих країн ЄС. Для прикладу, в США, крім офіційних, практикуються експертизи законопроектів з відомими та авторитетними недержавними інститутами, які володіють достатнім авторитетом і довірою парламенту, виконують цю функцію професійно та відповідально.

В Швейцарії оцінка законодавства входить в обов'язки парламенту, в багатьох законах і підзаконних актах містяться статті щодо подальшої періодичної оцінки їх дієвості. Важливо зауважити, що рішення ЕСПЛ на сьогодні не визнаються в Україні джерелами законодавства, що не виключає можливість їх використання як джерел права. Отже, на нашу думку, врахування аналізу практики ЄСПЛ щодо справ, для вдосконалення національного законодавства в напрямку зближення до міжнародних стандартів, а також усунунення недоліків національного законодавства, які спричинили порушення, що стали предметом розгляду. Цінною є участь представників громадянського суспільства, комерційної діяльності і науковців з огляду також на використання професійного досвіду, порівняльних досліджень та зарубіжного досвіду в законотворчому процесі. А питання інформаційної безпеки, як вже згадувались є надзвичайно динамічними і потребують значного обсягу професійних знань для розуміння не лише їх технологічної сторони, а й соціальних наслідків. Особливою уваги заслуговує питання правової культури та громадянської свідомості членів суспільства. Інструменти, що надає у руки громадянам,

інститутам громадянського суспільства і державним органам матимуть вплив за умови їх осмисленого використання усіма учасниками правовідносин. Електронна демократія і електронне урядування означає не лише оцифровування окремих документів та зміна каналів отримання інформації. Має відбутись переосмислення всіх процесів і цінностей в демократичному суспільстві. Таким чином, міжнародний досвід свідчить про дихотомію проблеми міжнародної інформаційної безпеки, та інформаційної безпеки людини як складової інституту прав людини в міжнародному праві. Узгодження основних питань є необхідним з огляду на економічні інтереси держав, демократичні цінності та глобалізаційні процеси, і, водночас, практично неможливим з огляду на розбіжності в інтересах основних геополітичних гравців.

При цьому правове та організаційне забезпечення інформаційної безпеки людини лише на національному рівні є недостатнім з огляду на глобалізацію, інтенсивні транскордонні інформаційні процеси, трудову міграцію, е-комерцію, втрату ідентичності та ще цілу низку соціальних процесів, що виникають у зв'язку зі становленням інформаційного суспільства. Український законодавець вже визначився з основним вектором зовнішньої політики, а, отже, законодавство в інформаційній сфері має відповідати цьому вектору. Враховуючи, що інформаційне законодавство України формувалось безсистемно і під впливом різних моделей правового регулювання інформаційної сфери, на сьогодні, важливим є опрацювання Інформаційного кодексу, який би відображав основні пріоритети, визначав систему і структуру інформаційного законодавства, водночас, залишаючи простір для реагування на динамічні процеси в інформаційній сфері.

З огляду на це, перспективними напрямами наукової розробки у досліджуваній предметній сфері вбачаються: захист прав людини на безпечне інформаційне середовище; правове забезпечення інформаційного суверенітету держави і суспільства; правове забезпечення освіти і науки в умовах глобалізації та розбудови інформаційного суспільства; правові засади захисту

персональних даних з урахуванням змін в законодавстві ЄС; процесуальні проблеми правозаствосовчої і правореалізаційної діяльності в інформаційній сфері; правове регулювання діяльності в сфері ІТ; правове регулювання діяльності суб'єктів системи забезпечення інформаційної безпеки, правові основи інформаційнопсихологічної безпеки людини; правове регулювання надання інформаційнопсихологічних послуг та психотерапевтичної допомоги; питання правового забезпечення інформаційної безпеки людини у зв'язку з використанням електронних реєстрів; правове регулювання використання генетичної інформації; правове забезпечення інформаційної безпеки людини в умовах використання інтернету речей, хмарних технологій, технології обробки великих даних, нейронних мереж, штучного інтелекту та робототехніки; юридична відповідальність за інформаційні делікти.

Таким чином, підходи до розуміння інформаційної безпеки людини в Україні та світі за роки зазнали суттєвих трансформацій, зокрема, сформувались політичні уявлення про місце цієї сфери в суспільному житті, роль держави в її регулюванні, розуміння мети і змісту державного управління інформаційною безпекою, механізмів державного впливу на інформаційні процеси та відносини. Відповідним чином змінювалося законодавство, структура та функції суб'єктів цієї політики.

Аналіз державної політики щодо інформаційної безпеки людини в Україні дозволив визначити, що інформаційна безпека людини є істотною частиною державної політики в переважній більшості напрямів, зокрема, зовнішньої політики, соціальної політики і політики в галузі прав людини, у сфері національної безпеки, у сфері охорони здоров'я і екологічної політики тощо. Таким чином, можна констатувати, що чинне законодавство не дає цілісного і системного закріплення офіційних поглядів, принципів, напрямів діяльності, спрямованих на реалізацію державної політики інформаційної безпеки людини. Водночас, аналіз правових основ державної політики дозволяє зробити висновок, що як окремий напрям державна політика інформаційної безпеки (в цілому, і людини, зокрема) не виділяється, хоча в науковій думці

існує такий підхід. З метою вдосконалення системи організаційного забезпечення та правового регулювання відносин у сфері інформаційної безпеки людини, які повинні базуватись на комплексному і системному підходах, запропоновано створити центральний орган виконавчої влади, що буде реалізовувати політику держави щодо розбудови приязного для людини інформаційного суспільства в Україні. До сфери відповідальності такого органу мають бути віднесені: координація розбудови інформаційної інфраструктури держави; забезпечення умов для реалізації інтересів людини, суспільства і держави в інформаційному просторі; координація діяльності інших державних органів в інформаційній сфері. Встановлення сутнісних ознак механізму правового регулювання відносин у сфері інформаційної безпеки людини, вбачається необхідним для визначення засад, на яких мають базуватись підходи щодо розробки та здійснення ефективного правового регулювання відносин у цій сфері. Оскільки інформаційна безпека є не лише самостійною сферою регулювання, а й невід'ємною складовою всіх інших – національної, екологічної, економічної, військової та інших, то її регулювання вимагає застосування єдиного системного підходу.

В його основу має бути покладено принцип найвищої цінності людини, гарантування її прав, свобод і законних інтересів. Окреслено загальну систему принципів правового регулювання інформаційних відносин, а також виокремлено специфічні принципи, що є визначальним для правових основ інформаційної безпеки людини, до яких запропоновано віднести: - принцип пріоритету прав, свобод і законних інтересів людини і громадянина; - принцип свободи інформації і обмеження доступу до інформації виключно у випадках передбачених законом; - принцип розвитку сприятливого для людини інформаційного суспільства; - принцип відповідальності держави перед людиною та суспільством за реалізацію державної політики інформаційної безпеки; - принцип мінімізації негативного інформаційного впливу на людину, в т.ч. шляхом формування інформаційної культури людини і суспільства; - принцип участі громадянського суспільства у розробці та контролю за

реалізацією заходів щодо попередження та захисту від загроз інформаційній безпеці людини; - принцип гармонізації інформаційного законодавства України із законодавством ЄС та положеннями міжнародного права у сфері інформаційної безпеки. Здійснено аналіз окремих видів актів застосування норм права у механізмі правового регулювання у сфері інформаційної безпеки людини. На його основі запропоновано уповноваженому із захисту прав людини, а в перспективі – Уповноваженому з інформаційної безпеки людини - надати відповідні повноваження щодо застосування норм права з метою припинення правопорушень та відновлення порушених прав. Також на основі аналізу судової практики у справах, що стосуються порушення прав людини на доступ до інформації, захисту персональних даних та інших інформаційних прав, обґрунтовано необхідність створення Вищого інформаційного суду. Пропозиції щодо вдосконалення українського законодавства у інформаційній сфері, насамперед, щодо інформаційної безпеки людини, сформовані на основі аналізу його розвитку, сучасного стану, досвіду іноземних держав та наукових досліджень.

Сучасний стан інформаційного законодавства характеризується невпорядкованістю, неузгодженістю та безсистемністю. Інформаційна сфера обслуговує практично всі аспекти суспільного життя – державотворення, безпеку, оборону, економіку, фінансову та грошову системи, соціальну сферу, екологію, науку, освіту і культуру, міжнародне співробітництво. Отже, інформаційна безпека виступає і як самостійна сфера регулювання, і є складовою всіх інших – національної, екологічної, економічної, військової та інших. Таким чином, законотворення у сфері інформаційної безпеки не може відбуватись відокремлено від розвитку системи права, частиною якого воно є. Розвиток законодавства у цій сфері вимагає ефективної співпраці органів державної влади, інститутів громадянського суспільства, комерційних структур і наукового потенціалу держави. Розробка законодавства щодо інформаційної безпеки людини вимагає створення ефективних механізмів активної участі у законотворчій діяльності її суб’єктів – належний доступ до проектів нормативних актів у цих сферах, реальні

публічні обговорення, а також врахування їх результатів. Актуальною проблемою залишається необхідність вироблення єдиних техніко-юридичних та мовно-термінологічних вимог до підготовки проектів законів у інформаційній сфері. Оскільки ця сфера відносно нова, надзвичайно динамічна і наукоємна, то й вимагає використання наукового потенціалу при розробці законопроектів у цій сфері, а також проведення експертного оцінювання ефективності вже існуючого законодавства. Особливої уваги заслуговує питання правової культури та громадянської свідомості членів суспільства. Нові інструменти, що надаються громадянам, інститутам громадянського суспільства і державним органам, матимуть вплив за умови їх осмисленого використання усіма учасниками правовідносин. Електронна демократія і електронне урядування означає не лише оцифровування окремих документів та зміну каналів отримання інформації, вони вимагають переосмислення всіх процесів і цінностей в демократичному суспільстві. Враховуючи, що інформаційне законодавство України формувалось безсистемно і під впливом різних моделей правового регулювання інформаційної сфери, на сьогодні, важливим є опрацювання базового закону – Інформаційного кодексу, який би відображав основні пріоритети, визначав систему і структуру інформаційного законодавства, водночас, залишаючи простір для реагування на динамічні процеси в інформаційній сфері. Врегулювання вимагає низка питань, що щільно пов’язані з інформаційною безпекою людини, які мають різний ступінь наукового опрацювання і сприйняття суспільством. Особливої уваги при нормотворенні вимагають ті, що не мають сформованої однозначної етичної оцінки, і тому значно складніше інтегруються у суспільну свідомість, отже, і в правову культуру.

Зокрема, йдеться про правове регулювання відносин, пов’язаних із використанням штучного інтелекту та робототехніки, технологій аналізу великих даних, політтехнологій, пропаганди та маніпуляцій суспільною свідомістю, використання генетичної інформації тощо. Вони безпосередньо пов’язані не лише з інформаційною безпекою людини, а й з безпекою людини в цілому, як фізичної особи і як члена суспільства.

ВИСНОВКИ

У монографії розглянуто та обгрунтовано важливу науково-прикладну проблему, що полягає в удосконаленні механізмів формування та реалізації державної інформаційної безпеки в Україні.

Одержані в процесі дослідження результати свідчать про реалізацію поставленої мети і завдань, дають можливість сформулювати загальні висновки та внести пропозиції, що мають теоретичне і практичне значення.

1. Доведено, що класичне визначення поняття «інформація» в його соціологічному аспекті доповнюється некласичним розумінням її соціально-економічної природи, що набуває під впливом глобалізаційних процесів якісно інших властивостей, стає ключовим при здобутті знань, формує уявлення про реалії соціальної дійсності й відтворює в цілому картину світу. Інформація має самостійну цінність, свої специфічні закономірності функціонування й розвитку, здатна до випереджального впливу на інформаційну політику, виступає безпосередньою причиною, що визначає вибір того або іншого варіанту політичного розвитку, поведінки різних соціальних груп і окремих громадян, переведення державної системи в новий стан. Інформація є вихідним ресурсом для розроблення інформаційної політики та здійснення державного управління в будь-якій сфері життєдіяльності суспільства й держави. На підставі зазначеного виокремлено сутнісні ознаки інформації як складової державної інформаційної політики: селективність – виникнення інформації зводиться до акту вибору, а нагромадження інформації – до результатів відповідних актів, тобто вибір, або в більш широкому сенсі – селективність, включається в поняття інформації як одна з його складових; субстанціональна несамостійність – властива як енергії, так і інформації, адже без будь-яких матеріальних носіїв немає ні енергії, ні інформації; спадкоємність – виділення й диференціація історичності й саморозвитку; масовість – розкриває зміст інформації як суспільної, загальної для всіх; цінність – за однакових

вірогідності та форми подання інформації її цінність не залежить від витрат на її отримання; трансформаційність – незалежність змісту інформації від форми її фіксації та способу розповсюдження; здатність до обмеження – чим вище рівень організованості системи, тим більше ступінь обмеження інформації; універсальність – зміст інформації може бути будь-яким; якість – сукупність властивостей інформації, що характеризують ступінь її відповідності до потреб (цілей, цінностей) користувачів.

2. Аналіз сучасних теоретико-методологічних підходів до змісту державної інформаційної політики доводить, що розширення національного інформаційного простору, різноманіття форм інформаційних процесів, каналів зв'язку визначають складність, багатоаспектність формування та реалізації державної інформаційної політики. При визначенні поняття «державна інформаційна політика» уявляється доцільним дотримуватися комплексного підходу, заснованого на міждисциплінарному синтезі та взаємодоповнюваності наукових методів. Доведено, що забезпечення державної інформаційної безпеки – це система цілеспрямованих, здійснюваних державою спільно з інститутами громадянського суспільства заходів адміністративно-управлінського характеру з регулювання інформаційних процесів, формування й розвитку інформаційного суспільства на основі пріоритету національних інтересів країни з метою захисту духовних і моральних цінностей, забезпечення інформаційної безпеки особистості, суспільства і самої держави, а також створення сприятливого економічного, соціокультурного та інформаційного середовища для гідних умов життя більшості громадян, гармонізації усіх сфер суспільства, досягнення стабільності та громадянської злагоди.

3. У сучасному інформаційному суспільстві складаються нові форми масової комунікації, соціального спілкування, стилі мислення і способи життя, нові парадигми економіки, політики, управління. Це потребує нового законодавчого закріплення сучасних принципів та функцій державної інформаційної політики. Відповідно до змістовних ознак поняття «державна інформаційна політика», сформовано групу принципів її формування –

принципи системності, повноти, об'єктивності, єдності кількості та якості інформації, науковості тощо, та функціонування – рівного доступу громадян країни до всіх джерел інформації, за винятком тих, володіння якими може зашкодити охороні державної та особистої таємниці, інтелектуальної власності; довіри громадян до ЗМІ і влади; єдності свободи слова та відповідальності за поширювану інформацію; зворотного зв'язку; перманентного вдосконалення інформаційного законодавства; урахування зарубіжного досвіду здійснення інформаційної політики та ін.

До базових принципів державної інформаційної політики можна віднести принципи: пріоритету національних, державних інтересів; урахування інтересів переважної більшості громадян; соціальної орієнтованості інформації; диференційованої державної підтримки недержавних ЗМІ; відкритості інформації; пріоритету вітчизняного виробника інформаційно-комунікаційних засобів, продуктів, послуг; урахування рівнів соціально-економічного, науково-технічного і культурного розвитку країни в цілому та її регіональних суб'єктів; єдності професійних і духовно-моральних якостей людей, які працюють у цій сфері; пріоритетного впливу держави з метою регулювання соціально-політичних і техніко-технологічних складових інформаційної політики й ін. Під функціями державної інформаційної політики розуміються дії держави, що сприяють підтриманню досягнутого стану та подальшому розвитку інформаційної сфери суспільства і його суб'єктів. Різноманіття зв'язків, що утворюють інформаційну сферу та взаємодії держави в ній, зумовлює низку функцій: інформаційну, освітню, гуманітарну, критики та контролю, артикуляції та інтеграції, мобілізаційну, адекватного реагування на іноземний інформаційно-психологічний вплив та ефективної протидії йому в сучасних умовах. Сфокусувавши увагу на характеристиці основних, провідних, з нашої точки зору, функцій державної інформаційної політики, зазначимо, що можна виділити й інші, наприклад: ініціативну, формування громадської думки, раціоналізації, гуманітарну тощо.

4. Перехід до гуманізованого інформаційного суспільства на практиці

неможливий без ефективної соціально спрямованої інформаційної політики. Це в свою чергу означає, що формування інформаційної політики органами державної влади має бути засноване на відповідних функціях і принципах, які реально характеризують її соціальну спрямованість. Соціально орієнтована державна інформаційна політика передбачає забезпечення реалізації найважливіших її соціальних функцій, серед яких інтеграційна, освітня, мобілізаційна, функція артикуляції інтересів, захисна, духовна тощо. Повна реалізація зазначених функцій можлива тільки в разі використання наукових принципів формування державної інформаційної політики, котрі враховують якісний аспект інформаційного розвитку. Як головні принципи можна виділити принципи цілісності інформаційного простору, системності, досягнення випереджального інформаційного ефекту, довіри, людяності, органічної єдності свободи та відповідальності тощо.

5. Доведено, що головними з пріоритетних напрямів формування та реалізації забезпечення державної інформаційної безпеки для органів державної влади повинні стати соціальна орієнтованість і соціальна відповідальність, соціально значуща суть явищ, процесів і факторів, котрі визначають зміст управлінських рішень, дії в будь-якому суспільстві та віддзеркалюють соціальні інтереси, цілі, настрої, потреби тих або інших соціальних верств, сприяють їхнім презентації й реалізації. Якість державної інформаційної політики визначається на основі критеріїв, показників та індикаторів, котрі дозволяють оцінити її відносно суб’єкта інформаційного обміну, виробництва інформації й управління нею, об’єкта дії та всіх елементів системи управління. Досконалою можна вважати лише таку інформаційну політику держави, функціонування та вплив якої сприяє оптимальному розвитку системи суспільних стосунків.

Доцільно виділити найбільш істотні напрями реалізації інформаційної політики держави: перший – формування й розвиток єдиного інформаційного простору України, що зумовлене як географічними, так і соціально-культурними відмінностями регіонів України; другий – розвиток інформаційно-комунікаційної інфраструктури; третій – формування умов, що сприяють

виробництву та використанню інформації і знань у всіх сферах життя суспільства; четвертий – розвиток інформаційного середовища як бази вдосконалення сфери державного управління; п’ятий – міжнародне співробітництво у сфері інформаційно-комунікативних технологій.

9. Реалізацію державної інформаційної політики України має бути спрямовано: на зміцнення Української держави на основі єдиного інформаційного простору країни; поглиблення процесів інформаційної та економічної інтеграції регіонів; створення сучасних мережевих структур державного, регіонального, міського управління та побудову на базі їх нових ефективних механізмів взаємодії влади з інститутами громадянського суспільства, бізнесом і населенням; становлення та в подальшому домінування в економіці нових технологічних укладів, що базуються на масовому використанні перспективних інформаційних технологій, засобів обчислювальної техніки і телекомунікацій; провідну роль інформаційно-комунікаційної інфраструктури в системі суспільного виробництва, у соціальній і культурній сферах; підвищення якості освіти, рівня науково-технічного і культурного розвитку за рахунок розширення можливостей інформаційного обміну на міжнародному, національному та регіональному рівні; підвищення ролі кваліфікації, професіоналізму і здібностей до творчості як найважливіших характеристик послуг праці, а також досягнення високого рівня мінімальної соціальної забезпеченості; створення ефективної системи забезпечення прав громадян і громадських інститутів на вільне отримання, розповсюдження й використання інформації як найважливішої умови демократичного розвитку; забезпечення високого рівня національної безпеки за рахунок запобігання терористичним і кримінальним загрозам в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамкин Г. П. Информатизация общества — итоги и перспективы [Электронный ресурс] / Г. П. Абрамкин — Режим доступа: http://aeli.altai.ru/conferenc/2000/abramkin.htm. — Загл. с экрана.

2. Авдиенко Д. А. Влияние в процессе политической коммуникации [Электронный ресурс] / Д. А. Авдиенко. — Режим доступа: http:// www.politjournal.spb.ru/120106.html. — Загл. с экрана.

3. Аверьянов В. Б. Аппарат государственного управления: содержание деятельности и организационные структуры / В. Б. Аверьянов. — Киев, 1990. — 145 с.

4. Авцинова Г.И. Информационная стратегия как фактор формирования политической культуры общества в условиях глобализации / Авцинова Г.И., Краснов Б.И., Лаптев Л.Г., Шелудько Л.В. — М., 2002. — С. 56.

5. Агамирзян И. Мировой опыт реализации концепции «электронного правительства» [Электронный ресурс] / И. Агамирзян. — Режим доступа: http://www/microsoft.com/rus/govemment/analytics. — Загл. с экрана.

6. Азроянц Э. А. Немарковские процессы как новая парадигма / Азроянц Э. А., Харитонов А. С., Шелепин Л. А. // Вопросы философии. — 1999. — С. 218.

7. Алмонд Г. А. Гражданская культура и стабильность демократии / Г. А. Алмонд, С. Верба // Полис. — 1992. — № 4. — С. 122–134.

8. Амоша О. Промислова політика України: концептуальні орієнтири на середньострокову перспективу / О. Амоша, В. Вишневський, Л. Збаразька // Економіка України. — 2009. — № 11. — С. 4–14.

9. Андрєєва О. М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією : [монографія] / О. М. Андрєєва ; НАН України, Ін-т політ. і етнонац. дослідж. ім. І. Ф. Кураса. — К. : Парлам. — 2009. — 359 с.

10. Андрийко О. Ф. Контроль в демократическом государстве: проблемы и тенденции / О. Ф. Андрийко. — Киев, 1994. — 165 с.

11. Андронова О. Электронное правительство в Европе и мире [Электронный ресурс] / О. Андронова, А. Николаев. — СПб., 2001. — Режим доступа: http://www.ci.ru/inform22_01/p_06oo.htm. — Загл. с экрана.

12. Анохин М. Г., Комаровский В. С. Информационные технологии в политике / Анохин М. Г., Комаровский В. С. // Политика: возможность современных технологий. — М., 1998. — С. 54.

13. Аппарат государственного управления: интересы и деятельность // [В. Ф. Сиренко, Н. В. Онищук, В. Б. Аверьянов и др.]. — К. : Наук. думка, 1993. — 165 с.

14. Аристотель. Политика. // Аристотель. Сочинения: В 4 т. — Т.4. — М., 1983. — С. 376.

15. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти [моногр.] / І.В. Арістова. — Харків: Вид-во Харк. нац. ун-ту внутр. справ, 2000. — 365 с.

16. Арістова І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики: Монографія. — Харків : Вид-во Харк. нац. ун-ту внутр. справ, 2006. — 256 с.

17. Арон Р. Демократия и тоталитаризм / Арон Р. — М.: Текст, 1993. — С. 21–22.

18. Арон Р. Измерения исторического сознания = Dimensions de la conscience historique / Р. Арон ; пер. с фр. И. А. Гобозова ; отв. ред. и авт. заключит. ст. И. А. Гобозов. — Изд. 2-е. — М. : ЛИБРОКОМ, 2010. — 185 с.

19. Арсеньев М. Н. Принятие решений. Интегрированные интеллектуальные системы : [учеб. Пособие для вузов] / М.

Н. Арсеньев, С. И. Шелобаев, Т. К. Давыдова. — М. : ЮНИТИ-ДАНА, 2008. — 270 с.

20. Артюшин Л. М. Теоретичні аспекти стратегії воєнної безпеки суспільства і держави / Л. М. Артюшин, Г. Ф. Костенко ; Нац. ун-т внутр. справ. — Х. : Вид-во НУВС, 2003. — 175 с.

а. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір : дис. …кандидата філософ. наук : 09.00.03 / НТУ України «Київський політехнічний інститут». К., 2012. 199 с. 19.Аскерко А. Комментарий к Закону Республики Беларусь «О регистре населения.» URL: http://www.center.gov.by/article61.html (дата звернення: 02.10.2017)

21. Атаманчук Г. В. Государственное управление: организационно-функциональные вопросы / Г. В. Атаманчук. — М. : ОАО НПО «Экономика», 2000. — 302 с.

22. Атаманчук Г. В. Управление: сущность, ценность, эффективность / Г. В. Атамчук. — М. : Культура : Акад. проект, 2006. — 542 с.

23. Атаманчук Г. Методологічні проблеми сучасного державного управління / Г. Атаманчук // Вісн. УАДУ. — 2001. — № 3. — С. 9–12.

24. Бабаев О. Я. Проблемы уголовно-правового регулирования в сфере компьютерной информации / Бабаев О. Я., Мещеряков В. А. // Защита информации. Конфидент. — 1998. — № 5 (23). — С. 67–73.

25. Бабец О. Опыт военной разведки на службе в коммерческой фирме / Бабец О. — М.: Харвест, 2004. — С. 42–47.

26. Базилюк Я. Б. Україна у системі міжнародної безпеки : монографія / Я. Б. Базилюк, О. С. Бодрук, Д. Ю. Венцковський [та ін.] ; Рада нац. безпеки і оборони України ; Нац. ін-т пробл. міжнар. безпеки. —К. : Фоліант, 2009. — 572 с.

27. Бакуменко В. Д. Загальні моделі уявлення суб'єкт-об'єктних відносин у соціальних системах / В. Д. Бакуменко // Актуальні проблеми державного управління : зб. наук. пр. Укр. акад. держ. упр. при Президентові України : Одеський філіал. — 2000. — Вип. 4. — С. 73–80.

28. Бакуменко В. Д. Теоретичні та організаційні засади державного управління / В. Д. Бакуменко, П. І. Надолішній : навч. посіб. —К. : Міленіум, 2003. — С. 8–11.

29. Бакуменко В. Д. Формування державно-управлінських рішень: проблеми теорії методології, практики: [моногр.] / В. Д. Бакуменко. — К. : Вид-во УАДУ, 2000. — 328 с.

30. Баранов О. Система принципів інформаційного права. Правова інформатика. 2006. № 2(10) с.5-11 26.Баранов О.А. Право власності на інформацію. Правова інформатика. 2008. № 1(17). С.15-19.

31. .Баранов О.А. Інформаційна безпека і економічні перетворення. Поглиблення ринкових реформ та стратегія економічного розвитку України до 2010 р.: Мат.міжнародної конференції. К., 1999. Ч. 2, т. 1. 168 с.

32. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи Київ: СофтПрес, 2005. 316 с.

33. Баранов О.А. Методи інформаційного права. Правова інформатика 2007. № 4(16). с.8-12. 30.Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: Моногр. Київ: Едельвейс, 2014. 434 с.

34. Баранов О.А. Правові проблеми “електронної демократії”. Інформація і право. 2017. № 1(20). с.28-38. 32.Бауман З. Глобалізація. Наслідки для людини і суспільства / пер. з англ. І. Андрущенка. К.: Вид. дім "Києво-Могилянська академія", 2008. 109 с.

35.Баринов А. Информационный суверенитет или информационная безопасность? / А. Баринов // Національна безпека і оборона. — 2001. — № 1. — С. 70–76.

36. Баровська А. В. Механізми реалізації державної інформаційної політики у сфері європейської інтеграції : автореф. дис. на здобуття наук. ступеня канд. держ. упр.: спец. 25.00.02 «Механізми державного управління» / А.В. Баровська. — Акад. муніціп. упр. — К., 2010. — 20 с.

37. Бачило И. Л. Актуальные проблемы информационного права / И. Л. Бачило // НТИ. Сер. 1, Орг. и методика информ. работы. — 2001. — № 9. — С. 3–8.

38. Бачило И. Л. Организационно-правовые проблемы информатизации / И. Л. Бачило // НТИ. Сер. 1, Орг. и методика информ. работы. — 1998. — № 3. — С. 13.

39. Бачило И.Л. Гражданское общество в зеркале Интернета. Массовая информация в Интернете: науч.-практ. конф. Москва, 12-13 октября 2007 г. URL: http://www.igpran.ru/about/subjects/center2/Konf/conference_abstracts.doc (дата звернення:11.08.2016) 34.Бачило И.Л. Информационное право. Основы практической інформатики: Учеб.пособ. М.: Юринформцентр, 2001. 352 с.

40. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учеб. СПб.: Юрид. центр Пресс, 2001. 789 с.

41. Бедрицкий А. А. Прав ли Президент Буш? / А. А. Бедрицкий // Независимое военное обозрение.12-18 октября 2001 г. — № 38. — С.4.

42. Беззубов Д.О. Суспільна безпека: (організаційно-правові засади забезпечення): Моногр. К.: МП Леся, 2013. 451 с.

43. .Безпека дітей в Інтернеті: відомості для батьків і вчителів URL:https://support.office.com/uk-ua/article (дата звернення: 02.10.2017) 412

44. .Безпека дітей в Інтернеті URL: http://mon.gov.ua/ua/activity/education/59/196/korinf19/bezditvinet/ (дата звернення: 02.10.2017) 39.Безпека інформації URL: http://jrnl.nau.edu.ua/index.php/Infosecurity (дата звернення: 10.09.2017)

45. Бек У. Общество риска. На пути к другому модерну / У. Бек. — М. : Прогресс–Традиция, 2000. — 384 с.

46. Белл Д. Возобновление истории в новом столетии : (предисл. к новому изд. кн. "Конец идеологии") / Д. Белл // Вопр. философии. — 2002. — № 5. — С. 13–25.

47. Белл Д. Грядущее постиндустриальное общество: Опыт социального прогнозирования: пер. с англ. / Д. Белл; В. Л. Иноземцев (ред. и вступ. ст.). — М. : Academia, 1999. — 956 с.

48. Белл Д. Социальные рамки информационного общества. Новая технократическая волна на Западе. М.: Прогресс, 1986. С. 330–342.

49. Беляева Е. В. Метаморфозы нравственности: динамика исторических систем нравственности. Минск: Экономпресс, 2007. 464 с.

50. Бєляков К.І., Ярмиш О.Н. Національна безпека України в інформаційній сфері: проблеми організаційного та правового забезпечення Безпекотворення: питання теорії і практики та правові аспекти : зб. наук.-практ. конф. (Київ, 16 лют.2007 р.): у 2 ч. Ч. 2 . К. : Вид-во Європ. ун-ту, 2007. С. 8–15.

51. Бєляков К., Ланде Д., Ніконова В. Інформаційне законодавство: новели 2013 р.. Юридчний Вісник України. № 52 (965). 28 грудня 2013 р. – 3 січня 2014 р.. с.14-15

52. Бєляков К.І. Знання про безпеку: проблеми визначення та методології. Боротьба з організованою злочинністю і корупцією (теорія і практика). К.: Міжвідомчий наук. дослід. центр, 2008. № 18. С.153-159. 413

53. Бєляков К.І. Інформація в праві: теорія і практика: Моногр. К.: КВІЦ, 2006. 118 с. 51.Бєляков К.І. Понятійні та методологічні основи регулювання нових типів інфор-маційних відносин : «віртуальні правовідносини». «Lex Portus». Одеса, Національний університет «Одеська юридична академія», 2016. № 2-2016. С. 47-63.

54. Бжезинский З. Великая шахматная доска (Господство Америки и его геостратегические императивы) / Бжезинский З. — М. : Международные отношения, 1998. — С. 98.

55. Биков В. Ю. Підвищення значущості інформаційно-комунікаційних технологій в освіті України / В. Ю. Биков // Педагогіка і психологія. — 2009. — № 1. — С. 28–33.

56. Битяк Ю. П. Державна служба в Україні: організаційно-правові засади : монографія / Ю. П. Битяк. — Х. : Право, 2005. — 304 с.

57. Битяк Ю. Проблеми визначення системи законодавства про державну службу / Ю. Битяк // Право України. — 2006. — № 5. — С. 22–26.

58. Біла К. Україна і загроза нової біполярності / К. Біла // Дослідження світової політики : зб. наук. пр. / Ін-т світової економіки і міжнар. відносин НАН України. — К., 2000. — С. 12–20.

59. Біла книга Держспецзв'язку. — Доступ : http://www.dsszzi.gov.ua

60. Біла С.О. Механізми впливу суспільства на державну інформаційну політику / С.О. Біла // Державне регулювання економічних процесів в уморах глобалізації. — Х.: С.А.М. — 2011. — С. 14–17.

61. Білорус О. Г. Глобалізація і безпека розвитку : [монографія] / О. Г. Білорус, Д. Г. Лук'яненко. — К. : КНЕУ, 2001. — 733 с.

62. Бінько І. Інформаційний простір України: стан та тенденції розвитку / І. Бінько // Бібл. вісн. — 2001. — № 2. — С. 15–18.

63. Бодрийяр Ж. Символический обмен и смерть / Ж. Бодрийяр. — М. : Добросвет, 2000. — 387 с.

64. Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти / О. С. Бодрук. — К. : Нац. ін-т пробл. міжнар. безпеки, 2001. — 300 с.

65. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. Актуальні проблеми післякризового відновлення економіки України:Зб. мат. наук.-прак. конференції викладацького складу і аспірантів навчально-наукового комплексу "Академія". Л., 2013.

66. Бодрук О.С. Структура воєнної безпеки: національний та міжнародний аспекти: Моногор. К.: НІПМБ, 2001. 300 с.

67. Бойко А. Розвиток інформаційних технологій — першочергове завдання державного управління / Андрій Бойко // Державне управління і право : зб. наук. пр. / Київ. нац. ун-т культури і мистец, Ін-т держ. упр. і права. — К., 2006. — Вип. 1, ч. 2. — С. 61–66.

68. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми / В. О.Бондаренко, О. В. Литвиненко // Стратег. панорама. — 1999. — № 1–2. — С. 127–133.

69. Бондаренко В. О. Інформаційні впливи і операції / В. О. Бондаренко, О. В. Литвиненко // Стратег. панорама. — 1999. — № 4. — С. 134–140.

70. Борисов В. І. Злочини проти безпеки виробництва: поняття та види. Кримінальна відповідальність за порушення правил ядерної або радіаційної безпеки : монографія / В. І. Борисов, О. О. Пащенко. — Х. : СПД Ф О Вапнярчук Н. М., 2006. — 224 с.

71. Бодрук О.С. Структура воєнної безпеки: національний та міжнародний аспекти: Моногор. К.: НІПМБ, 2001. 300 с.

72. Брандман Э. М. Глобализация и информационная безопасность общества: монография. М.: ГПИБ России, 2007. — С. 103.

73. Брауде-Золотарев М. Ю. Электронное государство и качество государственного управления / М. Ю. Брауде-Золотарев, В. В. Новиков // Интернет и современное общество : тр. X Всерос. объедин. конф., Санкт-Петербург, 23–25 окт. 2007 г. — СПб. : Фак. филологии и искусств СПбГУ, 2007. — С. 182–185.

74. Брижко В. Про приєднання України до Конвенції № 108 Ради Європи / В. Брижко // Право України. — 2003. — № 1. — С. 34–37.

75. Брижко В. До питання сучасної інформаційної політики. Вісн. Академії управління МВС. 2009. № 2. С. 32–36. 63.Брижко В. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. 2016. № 3(18). С. 45-57.

76. Брижко В.М. Захист персональних даних: реалії та практика сучасності. Інформація і право. 2013. № 3 (9). С. 31 – 49. 65.Булеца С. Персональні дані пацієнта розголосу не підлягають URL: http://yurincom.com/ua/legal_practice/analitychna_yurysprudentsiia/personalni_dani_patsiienta_rozgholosu_ne_pidliagaiut-publication/ (дата звернення: 11.10.2017)

77. Бриллюэн Л. Наука и теория информации / Л. Бриллюэн. — М. : Физматгиз, 1960. — 391 с.

78. Брокгауз Ф. А. Энциклопедический словарь. Современная версия / Брокгауз Ф. А., Ефрон И. А. — М.: Издательство Эксимо, 2004. — 672 с.

79. Брусницин Н. А. Информационная война и безопасность / Н. А.Брусницин. — М. : Вита-Пресс, 2001. — С. 69.

80. Бубенников А. Н. Япония на пороге XXI века: технологический, информационный вызов / Бубенников А.Н., Бубенников А.А. // Проблемы Дальнего Востока. 1999. — № 6. — С. 112–119.

81. Бурдье П. Социальное пространство: поля и практики : пер. с фр. / П. Бурдье ; сост., общ. ред. пер., послесл. Н. А. Шматко. — М. ; СПб. : Ин-т эксперимент. социологии : Алетейя, 2005. — 576 с.

82. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підр. / Бурячок В.Л. та ін..; за заг. ред. д.т.н., проф. В.Б. Толубка. К.: ДУТ, 2015. 288 с.

83. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannyata-perspektivi-spivpratsi-dlyaukrajini&catid=8&Itemid=350 (дата звернення:15.08.2017) 68.В ЛНР издали детский журнал Вежливые человечки URL: http://korrespondent.net/ukraine/3630876-v-lnr-yzdaly-detskyi-zhurnal-vezhlyvyechelovechky (дата звернення: 12.03.2016)

84. Бутко М. П. Інформаційно-аналітичне забезпечення діяльності органів виконавчої влади та місцевого самоврядування / М. П. Бутко // Наук.-техн. інформація. — 2002. — № 1. — С. 3–5.

85. Бучило И. Л. Информационное право: основы практической информации / И. Л. Бучило. — М., 2001 — С. 253.

86. Валлерстайн И. Анализ мировых систем и ситуация в современном мире / И. Валлерстайн ; пер с англ. П. М. Кудюкина ; под общей ред. Б. Ю. Кагарлицкого. — СПб. : Унив. кн., 2001. — 416 с.

87. Валлерстайн И. Конец знакомого мира. Социология XXI века / И. Валлерстайн. — М. : Логос, 2003. — 368 с.

88. Вартанова Е. Л. Современная медиаструктура / Е. Л. Вартанова // СМИ в постсоветской России. М., 2002. — С. 71.

89. Вахитов Р. Антииракская пропаганда: манипуляция сознанием / Р. Вахитов — Ресурс доступа: (www.patriotica.ru).

90. Вебер М. Политика как призвание и профессия // Вебер М. Избранные произведения. — М.: — Прогресс, 1990. — С. 646.

91. Вейманн Г. Как современные террористы используют Интернет / Г. Вейманн // www.crime-research. ru/analytics/Tropina_01/5.

92. Вепринцев В. Б. Операции информационно-психологической войны: методы, средства, технологии: Краткий энциклопедический словар / Вепринцев В. Б., Манойло А.В., Петренко А.И., Фролов Д.Б. М.: Горячая линия — Телеком, 2003. — С. 287.

93. Вернадский В. И. Биосфера и ноосфера / В. И. Вернадский. — М. : Айрис-Пресс, 2006. — 576 с.

94. Вернадский В. И. Научная мысль как планетное явление / В. И. Вернадский. — М. : Наука, 1991. — 270 с.

95. Вернадский В. И. О науке. Т. 1. Научное знание. Научное творчество. Научная мысль / В. И. Вернадского. — Дубна : Феникс, 1997. — 576 с.

96. Вернадский В. И. Философские мысли натуралиста : [сб. : к 125-летию со дня рождения] / В. И. Вернадский. — М. : Наука, 1988. — 519 с.

97. Видрін Д. Г. Україна на порозі XXI століття : політичний аспект / Д. Г. Видрін, Д. В. Табачник. — К. : Либідь, 1995. — 294 с.

98. Викторов С. Накануне 3-й мировой информационной войны / С. Викторов. — Финансовая Украина. — №5, 18 февраля 1997г.

99. Винер Н. Кибернетика и общество / Норберт Винер. — М. : Изд-во иностр. лит., 1958. — 200 с., (С. 31).

100. Винер Н. Кибернетика, или Управление и связь в животном и машине : пер. с англ. / Н. Винер. — 2-е изд. — М. : Наука, 1983. — 343 с.

101. Винер Н. Творец и робот: обсуждение некоторых проблем, в которых кибернетика сталкивается с религией / Норберт Винер; пер. с англ.: М. Н. Аронэ, Р. А. Фесенко. — М. : Прогресс, 1966. — 103 с.

102. Винер Н. Челевек управляющий / Винер Н. — СПб., —2001.— С.71–73.

103. Внедрение концепции «электронного правительства». Стратегия по автоматизации государственных служб [Электронный ресурс]. — Режим доступа: http://www.microsoft.com/rus/government/whitepapers/eGov_Strategy.asp. — Загл. с экрана.

104. Возженников А. В. Национальная безопасность: теория, политика, стратегия / А. В. Возженников. — М. : НПО «Модуль», 2000.

105. Володенков С. В. Информационно-психологические войны и массовое сознание / С. В. Володенков // Вестник Московского университета. — Серия 12. — Политические науки. 2003, № 3. — С. 130–136.

106. Волокитин А. В. Информационная безопасность и информационное законодательство / Волокитин А.В., Копылов В.А // Сб. НТИ. — Сер. 1. — 1996. — № 7. — С. 97.

107. Волченков И. Д. Разработка и реализация информационной политики органами государственной власти в Российской Федерации : автореф. дис. на соискание науч. степени канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологи / И. Д. Волченков. — М., 2008. — 20 с.

108. Волошина Н.М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. Сучасні інформаційні технології у сфері безпеки та оборони. 2010. № 2. С. 53-56.

і.Воронина Т. П. Информационное общество: сущность, черты, проблемы / Т. П. Воронина. — М., 1995. — 111 с.

109. Гаджиев К. С. Введение в политическую науку: Учебник для высших учебных заведений / К. С. Гаджиев. — М.: Логос, 1997. — С. 440.

110. Гаєвський Б. А., Ребкало В.А., Туленков М.В. Політичне управління: Навчальний посібник / Гаєвський Б. А., Ребкало В. А., Туленков М. В.— К.: Вид-во УАДУ, 2001— 160 с.

111. Галумов Э. Демиургические коды информации. Информация, информация, информация [Электронный ресурс] / Э. Галумов. — Режим доступа: http://contr-tv.ru. — Загл. с экрана.

112. Гарантувати безпеку/ Мова – ДНК нації. URL: https://ukrmova.in.ua/library/inshe/garantuvati-bezpeku (дата звернення: 04.03.2017) 83.Герасимова И. А. Диалог культур и когнитивная эволюция. Эволюция. Мышление. Сознание. М.: Канон, 2004. С. 169 -227

113. Гелбрейт Дж. К. Суспільство блага. Пора гуманності / Дж. К. Гелбрейт. — К. : Скарби, 2003. — 160 с.

114. Голіна В.В. Запобігання злочинності (теорія і практика): навч. посіб. Х.: Нац. юрид. акад. України, 2011. 120 с.

115. Головатий С. Верховенство права: Моногр. у 3-х кн. Київ: Вид-во «Фенікс», 2006. 1747 с.

116. Головенко Р. Право засобів масової інформації на поширення інформації як складова свободи слова. URL: http://ru.telekritika.ua/daidzhest/print/8620 (дата звернення: 10.05.2017)

117. Головенко Р.Б., Котляр Д.М., Слизьконіс Д.М. Доступ до публічної інформації:посібник із застосування «трискладового тесту». К.: ЦПСА, 2014. 152 с.

118. Головченко В. Правові механізми формування правосвідомості студентів. Право України. 2006. № 9. С. 100-103.

119. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. Вісник Київського університету імені Т. Шевченка.

1999. Вип.14: Міжнародні відносини. С. 46-48.

120. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу URL:https://dt.ua/internal/gibridna-viyna-yak-klyuchoviyinstrumentrosiyskoyi-geostrategiyi-revanshu-_.html (дата звернення: 04.03.2017)

121. Городенко Л.М. Цифрова та інформаційна нерівність у мережевій комунікації. 99.Государственные стратегии кибербезопасности URL: http://www.bezpeka.com/ru/lib/sec/gen/government-cybersecurity-strategy.html (дата звернення: 04.03.2017)

122. Грачев Г.В. Мельник И.К. Манипулирование личностью: Организация, способы и технологии информационно-психологического воздействия. М.: Алгоритм, 2002. 228 с.

123. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис. ... канд. юрид.наук: 25.00.02 / Національна академія державного управління при Президентові України. Київ, 2004. 22 с.

124. Гуцу С. Ф. Правові основи інформаційної діяльності: Навч. посібник Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін. -т», 2009. 48 с.

125. Гидденс Э. Устроение общества : очерк теории структурации / Э. Гидденс. — 2-е изд. — М. : Акад. Проект, 2005. — 528 с.

126. Гіденс Е. Нестримний світ: як глобалізація перетворює наше життя / Е. Гіденс; пер. з англ. Н. П. Поліщук. — К. : Альтерпрес, 2004. — 100 с.

127. Глазунова Н. И. Государственное и муниципальное (административное) управление: учеб. / Н. И.Глазунова. — М., 2007.— 469 с.

128. Глушков В. О. Організаційно-правові основи боротьби з тероризмом / В. О. Глушков, О. Ф. Долженков // Актуальні проблеми держави та права : зб. наук. пр. — О., 2000. — Вип. 8. — С. 73.

129. Гончаренко А. Н. Прогнозирование и политика : генезис и эволюция прогнозирования в системе национальной безопасности и

внешнеполитическом механизме США / А. Н. Гончаренко. — Киев : Наук. думка, 1993. — 188 с.

130. Горбулін В. П. Національна безпека: порядок денний для України / В. П. Горбулін, О. Ф. Бєлов, О. В. Литвиненко. — К. : Стилос, 2009. — 126 с.

131. Горбулін В. П. Системноконцептуальні засади стратегії національної безпеки України / В. П. Горбулін, А. Б. Качинський. — К.: ДП «Євроатлантикінформ», 2007. — 592 с.

132. Горбулін В. П. Актуальні проблеми системного забезпечення інформаційної безпеки України / В. П. Горбулін, М. М. Биченок, П. М. Копка // Матер. міжнар. наук.-практ. конф. «Форми та методи забезпечення інформаційної безпеки держави». — К. : Національна академія СБ України, 2008. — С. 79–85.

133. Горский Ю. М. Будущее цивилизации (экология, информация, экономика) / Ю. М. Горский, И. А. Кузнецова // Электротехника 2010 года : сб. докл. IV симп., Москва, 20–23 мая 1997 г. — Т. 1, разд. 6. — М., 1997. — С. 326–331.

134. Государственное управление: основы теории и организации : [учеб. пособие] / Под ред. В. А. Козбаненко. — М. : Статут, 2008. — 912 с.

135. Грачев Г. Манипулирование личностью / Грачев Г., Мельник И. — Режим доступа: http://vapp.ru/docs/manipul

136. Грачев Г. В. Информационно-психологическая безопасность личности: состояния и возможности психологической защиты / Г. В. Грачев— М.: — Изд-во РАГС, 1998. — С. 119.

137. Григор О. О. Формування інформаційного суспільства в Україні в контексті інтеграції в Європейський Союз (державно-управлінський аспект): автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр.: спец. 25.00.01 / Григор О. О.; Нац. акад. держ. упр. при Президентові України, Львів. регіон. ін-т держ. упр. — Л., 2003. — 20 с.

138. Григорьев М. С. Политические коммуникации в «век информации». //Политическое управление: Сборник научных трудов кафедры политологии и политического управления. — М.: Издательство РАГС, 1998

139. Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства. — Зарубежное военное обозрение. — № 8, 2001.

140. Губенков А. А. Информационная безопасность / А. А. Губенков, В. Б. Байбурин — М.: «Новый издательский дом», 2005. — 128 с.

141. Гудби Дж. Стратегия стабильного мира. Навстречу Евроатлантическому сообществу безопасности / Джеймс Гудби, Петрус Бувальда, Дмитрик Тренин. — М. : Междунар. отношения, 2003. —207 с.

142. Гуржеянц Т. В. Зарождение и развитие в США теории информационных войн // Информационные войны: мифы и реальность / Под ред. В.Д. Попоил, Е.П. Тавокина. — М., 2001. — С. 45.

143. Гурковський В. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання / В. Гурковський // Вісник УАДУ. — 2002. — № 3. — С. 27–32.

144. Гурне Б. Державне управління / Б. Гурне ; [пер. з фр.

145. Дайзард У. Наступление информационного века / У. Дайзард // Новая технократическая волна на Западе. — М. : Прогресс, 1986. — С. 343–354.

146. Данилишин Б. Новітні виміри сучасної практики соціально-економічних перетворень у державі / Б. Данилишин // Економіка України. — 2010. — № 8. — С. 40–50.

147. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації : навч. посіб. / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. — Х. : Фоліо, 2002. — 285 с.

148. Дарендорф Р. Современный социальный конфликт. Очерк политики свободы / Ральф Дарендорф ; пер. с нем. Л. Ю. Пантиной. — М. : РОССПЭН, 2002. — 284 с.

149. Дилс Р. Изменение убеждений с помощью НЛП. — М.: 1997.

150. Декларация принципов. Построение информационного общества — глобальная задача в новом тысячелетии // Всемирный Саммит по информационному обществу. — СПб., 2004. — С. 11–24.

151. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» від 12. 12. 2003 р.

152. Делінський О. А. Концептуальні аспекти становлення сучасної системи міжнародної безпеки / О. А. Делінський // Актуальні проблеми держави та права : зб. наук. пр. — О., 2001. — Вип. 11 : Правові проблеми становлення та розвитку сучасної Української держави : матеріали наук. конф. — С. 593–598.

153. Державне управління і менеджмент: навч. посіб. у табл. і схемах / Г. С. Одінцова [та ін.]; за заг. ред. Г. С. Одінцової. — Х. : ХарРІ УАДУ, 2002. — 492 с.

154. Дєгтяр А. О. Особливості стратегічного планування в органах державного управління / А. О. Дєгтяр // Актуальні проблеми державного управління: Зб. наук. праць. — Х. : Вид-во ХарРІ УАДУ «Магістр», 2002. — № 3(14). — С. 88 – 99.

155. Дєгтяр А. Підвищення якості державно-управлінських рішень щодо фінансово-кредитного регулювання аграрного сек- тора економіки України / А. Дєгтяр, В. Стрельцов, В. Черепанова // Актуальні проблеми державного управління : Зб. наук. праць. — Х. : Вид-во ХарРІ УАДУ «Магістр», 2003. — № 1(15). — С. 26 – 33.

156. Дзьобань О. П. Національна безпека України: концептуальні засади та світоглядний сенс / О. П. Дзьобань. — Х. : Майдан, 2007. — 284 с.

157. Дзюндзюк В. Б. Управлінські проблеми публічних організацій у світі, що змінюється / В.Б. Дзюндзюк // Зб. наук. праць Харківського регіонального інституту УАДУ при Президентові України “Актуальні проблеми державного управління”. — 2002.— №2. — Частина І. — С.158–161.

158. Дзюндзюк В. Б. Тенденції та перспективи європейської інтеграції України: державно-управлінські виміри: [Монографія] / За заг. ред. В.В. Корженко, Н.М. Мельтюхової. — Х.: ХарРі НАДУ, 2007. — 268 с.

159. Дзюндзюк В.Б. Віртуальні співтовариства: потенційна загроза для національної безпеки / В.Б. Дзюндзюк // Державне будівництво [Електронне видання]. — 2011. — Режим доступу до журн. : http://www.kbuapa.kharkov.ua

160. Демидов А. И., Федосеев А. А. Основы политологии. — М.: Высш. шк., 1995. — С. 145.

161. Доверие к СМИ в Украине. Інтернет-ресурс: Режим доступу. — http://institute.gorshenin.ua/researches/28_Doverie_k_SMI_v_Ukraine.html

162. Доценко Е. Л. Психология манипуляции. Феномены, механизмы, защита / Е. Л. Доценко — М. : МГУ, 1996. — 342 с.

163. Друкер П. Ф. Управление, нацеленное на результаты: [пер. с англ.] / Питер Ф. Друкер. — М. : Технол. шк. бизнеса, 1994. — 191 с.

164. Дридзе Т. М. Язык и социальная психология / Т. М. Дридзе; под ред. А. А. Леонтьева. — М. : Либроком, 2009. — 224 с.: ил.

165. Дубров Д. В. Основи електронного урядування : навч. посіб. / Д. В. Дубров, С. В. Дуброва. — К. : Центр навч. л-ри, 2006. — 176 с.

166. Дубровский Д. И Проблема идеального. Субъективная реальность / Д. И. Дубровский . — Канон, 2002. — 228 с.

167. Емельянов В. П. Терроризм и преступления террористической направленности / В. П. Емельянов. — Харьков : Рубикон, 1997. — 176 с.

168. Емельяненко О.М. Електронний уряд: інноваційні підходи до політики і управління в інформаційному суспільстві, 2008.

169. Жуков В. Взгляды военного руководства США на ведение информационной войны. — Зарубежное военное обозрение. № 1, 2001.

170. Закон України «Про доступ до публічної інформації» Режим доступу: kmu.gov.ua›Урядовий портал›/publish/article?art_id

171. Закон України « Про науково-технічну інформацію» від 25 червня 1993 року // Відомості Верховної Ради, 1993. — № 33. — ст. 345.

172. Закон України «Про Концепцію Національної програми інформатизації» // із змінами, внесеними згідно із Законом № 3421–IV (3421–15) від 09.02.2006. — № 22. — ст. 199.

173. Закон України «Про державну таємницю» : від 21 січ. 1994 р. № 3855 // Відом. Верховної Ради України. — 1994. — № 16. — Ст. 93.

174. Закон України «Про Загальнодержавну програму «Електронна Україна» на 2005–2012 роки» [Електронний ресурс]: проект від 15.04.2004 р. №5414. — Режим доступу: http://search.ligazakon.ua/1_doc2.nsf/link1/ed_2004_04_15/ID46EOOA.html# — Назва з екрана.

175. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»: від 31 трав. 2005 р. — № 2594 // Відом. Верховної Ради України. — 2005. — № 26. — Ст. 347.

176. Закон України «Про інформацію»: від 2 жовт. 1992 р. — № 2657 // Відом. Верховної Ради України. — 1992. — № 48. — Ст. 650., зі змінами згідно Закону України від 13.01.2011 р. № 2938-VI «Про внесення змін до Закону України «Про інформацію».

177. Закон України «Про Концепцію Національної програми інформатизації»: від 4 лют. 1998 р. — № 75 (із змінами, внесеними згідно з Законом України від 9 лют. 2006 р. № 3421) // Відом. Верховної Ради України. — 1998. — № 27/28. — Ст. 182.

178. Закон України «Про електронні документи та електронний документообіг» : від 22 трав. 2003 р. № 851 // Відом. Верховної Ради України. — 2003. — № 36. — Ст. 275.

179. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. — 2003. — № 39. — ст. 351.

180. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» : від 9 січ. 2007 р. — № 537 // Відом. Верховної Ради України. — 2007. — № 12. — Ст. 102.

181. Закон України «Про телекомунікації» // Відомості Верховної Ради України. — 2004. — № 12. — Ст. 155.

182. Закон України «Про оборону України» в редакції Закону від 11 травня 2007 року N 1014-V.

183. Закон України «Про Національну програму інформатизації» (Відомості Верховної Ради (ВВР), 1998, № 27–28, ст.181, із змінами, внесеними згідно із Законом № 2684-III від 13.09.2001, ВВР, 2002, № 1, ст.3).

184. Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» { Відомості Верховної Ради України (ВВР), 2006, N 13, ст.109 }.

185. Засурский Я. Н. Информационное общество в России: парадоксы Интернета // Информационное общество. — 2003. — № 5. — С. 40.

186. Звіт Генеральному секретарю ООН групи радників з інформаційних технологій: «Глобальна ініціатива щодо подолання інформаційної нерівності», ел. ресурс: buklib.net›component/option,com_jbook/task,view/…

187. Зуев С. Э. Измерения информационного пространства (политики, технологии, возможности) // Музеи будущего: информационный менеджмент / Сост. А. В. Лебедев. — М., 2001.

188. Засурский И. И. Ре-конструкция России. Масс-медиа и политика в России девяностых / И. И. Засурский — 2000. — Электронный ресурс: old.russ.ru›politics / 20001114_0.html.

189. Ингарден Р. Введение в феноменологию Эдмунда Гуссерля : лекции 1967 г. в Осло / Р. Ингарден ; пер. с норвеж.: А. Денежкин, В. Куренной. — М. : Дом интеллект. книги, 1999. — 224 с.

190. Информационная политика. Учебник. / По общей ред. В.Д. Попова. — М.: Изд-во РАГС, 2003. — С.318–331.

191. Информационное общество. Информационные войны. Информационное управление. Информационная безопасность / Под ред. М.А. Вуса. — СП б., 1999.

192. Информационное пространство Украины. Общая характеристика. Інтернет-ресурс: Режим доступу. – http://www.rb.com.ua/rus/analitics/socyum/7252/

193. Информационное пространство Украины: Основные каналы массовой коммуникации: Інтернет–ресурс: Режим доступу. – http://www.rb.com.ua/rus/analitics/socyum/7255/

194. Интервью Сергея Дороненко «Эхо Москвы» режим доступа: internet-radio.com.ua›archives/257.

195. Информационные вызовы национальной и международной безопасности / Под общ. ред. А.В. Федорова и В.Н. Цыгичко. — М.: ПИР–Центр, 2001;

196. Истон Д. Категории системного анализа политики / Д. Истон // Политология : хрестоматия. / [сост.: М. А. Василик, М. С. Вершинин]. — М. : Гардарики, 2000. — С. 319–331.

197. Истон Д. Категории системного анализа политики // Антология мировой политической мысли. В 5 т. — Т. 2. М. : Мысль, 1997.

198. Ібрагімова І. Інформаційне суспільство та взаємодія влади з громадськістю: вимоги ефективності / І. Ібрагімова // Вісн. НАДУ. — 2004. — № 1. — С. 36–42.

199. Іванов В. Захист суспільної моралі у засобах масової інформації / В. Іванов // Вісн. Нац. ради України з питань телебачення і радіомовлення. — 2002. — № 4. — С. 15–20.

200. Ільченко Н. М. Механізми реалізації державної політики у сфері засобів масової інформації (регіональний рівень), 2008.

201. Інформаційна безпека України. Проблеми і шляхи вирішення. Заочний круглий стіл // Національна безпека і оборона. — 2001. — № 1. — С. 24–29.

202. Інформаційні технології в регіональному управлінні: Нав. посіб./ Бутко М. П., Бутко І. М., Дітківська М. Ю. та ін. – К.: Знання України, 2006. — 282 с.

203. Кадымов С. Т. Проблемы государственного управления в современной России. Автореферат диссертации на соискание ученой степени кандидата политических наук. — М.: МГУ, 1998;

204. Казанцев В. О. Приоритетные национальные проекты / Вадим Казанцев. — М., 2007. — С. 52.

205. Кальниш Ю.Г. Громадська думка та експертні оцінки щодо напрямів і перспектив світової інтеграції України: політичний аналіз / Ю.Г. Кальниш // Наук. журн. “Менеджер” Вісн. Донець. держ. ун-ту упр. — 2006. — Вип. 3 (37). — С. 36–43.

206. Кара-Мурза С. Г. Манипуляция сознанием / С. Г. Кара-Мурза — М., 2007. — 728 с.

207. Кара-Мурза С. Г. Манипуляция сознанием. Учебное пособие / С. Г. Кара-Мурза. — М.: Алгоритм, 2004. — С.238.

208. Картавцев В. С. Кримінальна відповідальність за злочин проти основ національної безпеки України (наукові засади кваліфікації) : [навч. посіб.] / В. С. Картавцев. — К. : Нац. акад. СБ України, 2004. — 57 с.

209. Картунов О. Концепції прав людини та етнонаціональних меншин : від конфлікту до компромісу / Олексій Картунов // Політ. менеджмент. — 2005. — № 2. — С. 3–23.

210. Кастельс М. Галактика Интернет : Размышления об Интернете, бизнесе и обществе / пер. с англ. А. Матвеева ; под ред. В. Харитонова. — Екатеринбург : У-Фактория (при участии Гуманитарного ун-та), 2004. — 328 с.

211. Кастельс М. Информационная эпоха: экономика, общество и культура / Мануэль Кастельс ; пер. с англ. [Б. Э. Верпаховский и др.], под науч. ред. О. И. Шкаратана ; Гос. ун-т Высш. шк. экономики. — М.: Г У ВШЭ, 2000. — 606 с. : ил.

212. Кастельс М. Становление общества сетевых структур. Новая постиндустриальная волна на Западе: Антология. / Под ред. В. Л. Иноземцева. — М., 1990. — С.494.

213. Качинський А. Комплексна оцінка ризиків і загроз за складовими державної політики національної безпеки України / А. Качинський // Євроатлантикінформ : наук.-аналіт. бюл. Нац. центру з питань євроатлант. інтеграції України. — 2006. — № 5. — С. 55–61.

214. Кашлев Ю. Б. и др. Информация, массовая коммуникация и международные отношения. — М., 2005. — С. 40.

215. Ківалов С. В. Митна політика та національна безпека / С. В. Ківалов, Б. А. Кормич // Митна справа. — 2001. — № 4. — С. 3–14.

216. Клименко І. Б. Роль політичних партій у впровадженні гендерної рівності на Україні / І. Б. Клименко // Пробл. освіти. — 2003. — Вип. 30. — С. 250–262.

217. Клименко І. В. Технології електронного врядування / І. В. Клименко, К. О. Линьок. — К. : Центр сприяння інституційному розвитку державної служби, 2006. — 192 с.

218. Князєв В. М. Програмно-цільовий підхід до наукового Забезпечення реформи державного управління: дослідження, технології, методики / В. М. Князєв, В. Д. Бакуменко, Є. О. Рал- дугін, Ю. В. Бакаєв / За заг. ред. В. М. Князєва. — К. : Вид-во УАДУ. — 1999. — С. 17 – 28.

219. Князєв В. М. Філософсько-методологічні засади державно-управлінських рішень / В. М. Князєв // Вісн. УАДУ. — 2000. — № 2. — С. 341–358.

220. Коваль Р. А. Інформаційно-аналітичне забезпечення діяльності органів влади [Текст]: автореф. дис. канд. наук з держ. управління: спец. 25.00.02. — Харків. — 2008. — 20 с.

221. Ковальський В. П. Безпека України та вплив на неї воєнно-політичного оточення / В. П. Ковальський, О. Я. Маначинський, Є. К. Пронкін. — К., 1993. — 35 с.

222. Колодюк А. В. Теоретичне обґрунтування поняття та виникнення інформаційного суспільства / Колодюк А. В. // Борисфен. — 2004. — № 11. — С. 18–19.

223. Кольев А. Н. Политическая мифология: Реализация социального опыта / Кольев А. Н. — М., 2003. — С. 59.

224. Комов С. А. Информационная борьба в современной войне: вопросы теории / Комов С. А. // Военная мысль. — 1996, №3. — С.77–80.

225. Конвенція про захист прав людини та основних свобод із поправками, внесеними відповідно до положень Протоколу №11 // Практика Європейського суду з прав людини. — 1999. — №1.

226. Конвенція про кіберзлочинність (Закон від 07.09.2005 № 2824-IV)

227. Калинина А.Э. Развитие информационного пространства региональной хозяйственной системы / А.Э. Калинина. – Волгоград: Изд-во ВолГУ, 2005. — С. 14–26.

228. Конституція України : від 28 черв. 1996 р. // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.

229. Копан О. В. Забезпечення внутрішньої безпеки України: теоретико-управлінські засади. Введення в поліцейську стратегію : монографія / О. В. Копан. — К. : НАВСУ, 2001. — 424 с.

230. Князева Е.Н. Синергетика как новое миропонимание: диалог с И. Пригожиным / Князева Е.Н., Курдюмов С.П. // Вопросы философии. 1992. — №12.

231. Корецький М. Х. Система інформаційно-аналітичного забезпечення комплексного територіального розвитку й управління земельними ресурсами / М. Х. Корецький // Управління сучасним містом. — № 1–3 (9). — К. : УАДУ, 2003. — С. 66 – 70.

232. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посібник / Кормич Б. А. — К. : Кондор, 2004. — 384 с.

233. Косевцов В. О. Національна безпека України: проблеми та шляхи реалізації пріоритетних національних інтересів / В. О. Косевцов, І. Ф. Бінько ,

Рада нац. безпеки і оборони України, Нац. ін-т стратег. дослідж. — К., 1996. — 54 с.

234. Костенко Г. Ф. Теоретичні аспекти стратегії національної безпеки : навч. посіб. / Г. Ф. Костенко ; Дипломат. акад. України при М-ві закордонних справ України. — К. : ДЕМІД, 2002. — 144 с.

235. Костин Н. А. Общие основы теории информационной борьбы / Костин Н. А. // Военная мысль, 1997, №3. — С.44–50.

236. Костирєв А. Г. Роль засобів масової інформації в процесі демократичного розвитку суспільства : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 «Політ. ін-ти та процеси» / А. Г. Костирєв ; Київ. нац. ун-т ім. Т. Шевченка. — К., 2003. — 20 с.

237. Краткая философская энциклопедия. — М. : Прогресс-Энциклопедия, 1994. — 576 с.

238. Крок Л. Психологическое воздействие терроризма / Л. Крок // www.ruj.ru/smi-teror_2.htm.

239. Круть П. П. Концепція національної безпеки України: методологічний аспект / П. П. Круть // Актуальні проблеми сучасної науки в дослідженнях молодих учених : зб. наук. пр. — Х., 1997. — Вип. 2. — С. 73–79.

240. Крылов В. В. Информационные компьютерные преступления / Крылов В. В. — М. : ИНФРА-М-НОРМА, 1997. — С. 86.

241. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / Крысько В. Г. — Мн.: Харвест, 1999. — С. 49.

242. Крюков О. І. Громадянське суспільство як чинник побудови демократичної політичної системи / О. І. Крюков // Стратегічні пріоритети : наук.-аналіт. щокв. зб. / Нац. ін-т стратег. дослідж. ; [голов. ред. Рубан Ю. Г.]. — К. : Санспарель, 2009. — № 2. — С. 55–59.

243. Кузьменко Б. В. Захист інформації. Ч. 1. Організаційно-правові засоби забезпечення інформаційної безпеки / Б. В. Кузьменко, О. А. Чайковська. — К. : Вид. відділ КНУКІМ, 2009. — 83 с.

244. Кун Т. Структура научных революций / Кун Т. — М., 1975. — С. 11.

245. Курносов Ю. В. Аналитика: методология, технология и организация информационно-аналитической работы / Курносов Ю. В., Конотопов П. Ю. — М., 2004. — 512 с.

246. Курушин В. Д. Компьютерные преступления и информационная безопасность./ В. Д. Курушин, В. А. Минаев. — М.: Новый юрист, 1998. — С. 23.

247. Кухта Б. Л. З історії української політичної думки : текст лекцій : навч. посіб. / Б. Л. Кухта. — К. : Генеза, 1994. — 368 с.

248. Куц Ю. О. Підвищення ролі територіальної громади через механізм удосконалення системи місцевого самоврядування / Ю. О. Куц // Харківський регіон: пошук стратегії оптимального розвитку. — Х., 2006. — С. 9–11.

249. Кушнарев Ф. Ю. Информационная политика государственных органов управления как объект политического анализа: Матер.Всерос. науч.практич. конф. аналитических работников / Кушнарев Ф. Ю. // Власть. — 2004. — М 8. — С. 50.

250. Лашкина М. Г. Концептуальні засади взаємодії органів державної влади та засобів масової інформації в умовах демократизації / Лашкина М. Г. — 2008.— С. 214.

251. Лебедева М. М. Мировая политика / М. М. Лебедева — М., 2002.— С. 55.

252. Лебон Г. Психология толп. Кн. 2. Психология масс / Лебон Г. — М., 1998. — С. 26.

253. Левицька М. Б. Тероризм як загроза міжнародній і національній безпеці України / М. Б. Левицька // Актуальні проблеми держави та права : зб. наук. пр. — К., 2000. — Вип. 8. — С. 219–224.

254. Лесечко М. Д. Технологія прийняття управлінських рішень у державному управлінні та місцевому самоврядуванні: [навч. посіб.] / М.

Д. Лесечко, А. О. Чемерис, Р. М. Рудницька / за наук. ред. М. Д. Лесечка. – Львів : ЛРІДУ УАДУ, 2003. — 424 с.

255. Лопатин В. Н. Информационная безопасность России: человек, общество, государство / В. Н. Лопатин. — М., 2000.

256. Лисичкин В. Третья мировая информационно-психологическая война / Лисичкин В., Шелепин Л. — М, 1999. — С. 217.

257. Лисичкин В.А. Глобальная империя зла / В. А. Лисичкин, Л. А. Шелепин — М.: «Крымский мост-9Д», 2001. — С. 22.

258. Литвак О. М. Служба Безпеки України / О. М. Литвак. — К. : Юрінком-Інтер, 2000.

259. Литвиненко О. В. Національна безпека: порядок денний для України / О. В. Литвиненко, В. П. Горбулін, О. Ф. Бєлов. — К. : Стилос, 2009. — 126 с.

260. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. — К. : КНТ, 2006. — 280 с.

261. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади [Текст]: автореф. дис. канд. юридичних наук. — спец. 12.00.07 «Теорія управління; адміністративне право і процес;фінансове право; інформаційне право» / Логінов О. В. — Київ. — 2005. — 20 с.

262. Логінов О. В. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління / О. В. Логінов // Науковий вісник Юридичної академії МВС України. — 2003. — № 3. — С. 199–205.

263. Лопатин В. Н. Информационная безопасность в системе государственного управления: Теоретические и организационно-правовые проблемы: дис. канд. юридичних наук. — спец. 12.00.02 / Лопатин В. Н. — СПб., 1997. — 193 с.

264. Луговий В. І. Десять років становлення (дослід досліджень, розробок і впроваджень у сфері державного управління) / Луговий В. І. — К.: Вид-во НАДУ, 2005.— 356 с.

265. Лукьяненко А. Е. Персонал государственного аппарата: проблемы управления и стабилизации (социально-политический аспект). автореф. дис. на соискание ученой степени доктора социологических наук / А. Е. Лукьяненко. — М.: Институт социально-политических исследований РАН, 1998. — 20 с.

266. Луман Н. Медиа-коммуникации / Никлас Луман ; пер. с нем.: А. Глухов, О. Никифоров. — М. : Логос, 2005. — 280 с.

267. Луман Н. Общество как социальная система / Никла Луман ; пер с нем. А. Антоновского. — М. : Логос, 2004. — 232 с.

268. Луман Н. Реальность масс-медиа / Никлас Луман ; [пер. с нем. А. Антоновского]. — М. : Праксис, 2005. — 253 с.

269. Луман Н. Самоописания: общество общества / Никлас Луман ; [пер. с нем. под ред. О. Никифорова и А. Антоновского]. — М. : Логос ; Гнозис, 2009. — 318 с.

270. Луман Н. Социальные системы : очерк общей теории / Н. Луман ; пер. с нем. И. Д. Газиева ; под ред. Н. А. Головина. — СПб. : Наука, 2007. — 648 с.

271. Луман Н. Эволюция / Никлас Луман ; [пер. с нем. А. Антоновский]. — М. : Логос, 2005. — 254 с.

272. Луман, Н. Дифференциация./ Никлас Луман. — М. : Логос, 2006. — 320 с.

273. Макаренко Є. Інформаційна безпека України в контексті сучасних викликів та загроз / Євгенія Макаренко // Освіта регіону. Політологія, психологія, комунікації. — 2009. — № 1. — С. 86–94.

274. Манойло А В Информационно-психологическая безопасность современного информационного общества / А. В. Манойло, А. И. Петренко.: — М,: Стратегическая стабильность №3. — 2003г. — С. 59–64.

275. Манойло А В. Информационное противоборство и государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко. — М.: Правой политика, 2003. — № 9.— С 110–125.

276. Манойло А В. Государственная информационная политика в условиях информационно-психологической войны: [монография] / Манойло А В.. Петренко А. И., Фролов Д. Б // М. Горячая линия –Телеком. 2003 г. — 541 с . ил.

277. Манойло А. В. Информационно-психологические операции как организационная форма реализации концепции информационно-психологической войны / Манойло А. В. Фролов Д. Б., // Проблемы информационной безопасности. Компьютерные системы. 2003 г.— № 2.— С. 7–14.

278. Манойло А. В. Государственная информационная политика в особых условиях: [Монография] / А. В. Манойло. — М.: МИФИ, 2003. — 388 с.

279. Манойло А. В. Информационная война как инструмент внешней агрессии и территориальной экспансии. Учебное пособие / А. В. Манойло — М: НИИПИ, 2000.— С. 265.

280. Манойло А. В. Объекты и субъекты информационного противоборства / Манойло А. В. — Режим допуска: www .psyfactor.org

281. Манойло А. В. Особенности информационной политики эпохи информационного общества / А. В. Манойло, Д. Б. Фролов, В. Б. Вепринцев // Проблемы информационной безопасности. Компьютерные системы. — 2002. — № 4.

282. Мартин Г. П., Шуман Х. Западня глобализации: атака на процветание и демократию / Мартин Г. П., Шуман Х. — М., 2001.— С. 86.

283. Маркелов К. В. Информационные процессы: взаимодействие сознательною и бессознательного / К. В. Маркелов // Государственная информационная политика: концепции и перспективы: Сб. статей / Отв. ред. Е.П. Тавокин. М., 2001. — С. 69–70.

284. Марков М. Теория социального управления / М. Марков. — М. : Прогресс, 2008. — 448 с.

285. Мартиненко В. М. Інноваційна стратегія демократичного розвитку України: від місцевої демократії до демократичної держави : [монографія] / В. М. Мартиненко. — Х. : Константа, 2004. — 225 с.

286. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності : навч. посіб. / А. І. Марущак. — К. : Видавничий дім «Скіф»: КНТ, 2008. — 344 с.

287. Марущак А. І. Інформаційне право: Доступ до інформації: Навчальний посібник / А. І. Марущак. — К.: КНТ, 2007. — 532 с.

288. Маршалл М. Понимание медиа: внешние расширения человека = Understanding Media: The Extensions of Man / Маклюэн Маршалл. — М. : Кучково поле, 2007. — 464 с.

289. Матвієнко О. Концепція менеджменту інформаційних систем у контексті загальних проблем інформатизації суспільства / О. Матвієнко // Вісн. Кн. палати, 2002.— № 10.— С. 17–20.

290. Махлуп Ф Культурное разнообразие в изучении информации / Фриц Махлуп, Уна Мэнсфилд // Междунар. форум по информ. — 2004. — Т. 29, № 1. — С. 9–36.

291. Махлуп Ф Семантические изыски в изучении информации / Фриц Махлуп // Междунар. форум по информ. — 2004. — Т. 29, № 3. — С. 3–20.

292. Мелюхин И. С. Информационное общество: истоки, проблемы, тенденции развития / И. С. Мелюхин, МГУ им. М. В. Ломоносова, Фак. журналистики. — М.: Изд-во Моск ун-та, 1999. — 206 с.

293. Мельников О. Ф. Автоматизація і застосування комп’ютерних технологій в управлінській діяльності / О. Ф. Мельников // Актуальні питання організації навчання і методики викладання в системі підвищення кваліфікації державних службовців : матеріали міжнар. наук.-практ. конф. – К. : УАДУ, 1998. – С. 144 – 150.

294. Мерзляк А. В. Інформаційні системи та інформаційне забезпечення

державного управління / А. В. Мерзляк // Зб. наук. пр. ДонДУУ: «Управління діяльністю органів державної влади». — Серія «Державне управління» — Т.VII — Вип.71 — Донецьк 2009. — С 109–117.

295. Модестов С. А. Информационное противоборство как фактор геополитической конкуренции / Модестов С. А. — М.: Издательский центр учебных и научных программ, 1998.— С. 79.

296. Моль А. Социодинамика культуры / Моль А. — М., 1973. — С. 56.

297. Московичи С. Век толп. Исторический трактат по психологии масс / Московичи С. — М., 2001.— С. 22.

298. Назаров М. М. Массовые коммуникации и виртуализация социального пространства в современном обществе / М. М. Назаров // Соц.-гуманитар. знания. — 2001. — № 1. — С. 233–247.

299. Нейсбит Дж. Высокая технология, глубокая гуманность. Технологии и наши поиски смысла / Джон Нейсбит. — М. : АСТ : Транзиткнига, 2005. — 384 с.

300. Ненашев А. И. Средства электронной коммуникации в структуре социума / А. И. Ненашев. — Саратов : ФГОУ ВПО «Саратовский ГАУ», 2008. — 108 с.

301. Несвіт В. Ефективне використання оборотних коштів на підприємстві / Володимир Несвіт // Схід. — 2007. — № 1. — С. 30–33.

302. Несвіт Г.П. Інформаційна політика держави як чинник реформування суспільства / Несвіт Г.П. — 2001.— 235 с.

303. Нижник І. Формування рішень органами державного управління / І. Нижник, С. Мосов // Вісник НАДУ. — 2000. —№ 2. — С. 13 – 18.

304. Нижник Н. Р. Государственные управленческие отношения в демократическом обществе / Н. Р. Нижник / Ин-т государства и права НАН Украины. — К., 1995. — 207 с.

305. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. для вищих навч. закл. / Н. Р. Нижник,

Г. П. Ситник, В. Т. Білоус ; Укр. Акад. держ. упр. при Президентові України, Акад. держ. податк. служби України. — К. : Преса України, 2000. — 304 с.

306. Нижник Н. Р. Системний підхід в організації державного управління : [навч. посіб.] / Н. Р. Нижник, О. А. Машков ;за заг. ред. Н. Р. Нижник. — К. : Вид-во НАДУ, 1998. — 160 с.

307. Нижник Н. Управлінська культура: теоретичне поняття чи управлінська поведінка? / Ніна Нижник, Людмила Пашко // Політ. менеджмент. — 2005. — № 5. — С. 103–113.

308. Никитов В. Л. Информатизация парламентской деятельности США, Канады и государств Европы / Никитов В. Л., Орлов Е. И. // Сб. НТИ. Сер. 1. — 1996. — № 7.

309. Нисневич Ю. А. Государственное управление и информационная политика / Ю. А. Нисневич // НТИ. Сер. 1, Орг. и методика информ. работы. — 2000. — № 4. — С. 9–12.

310. Нисневич Ю. А. Информационно-коммуникационная стабилизация политической системы / Ю. А. Нисневич // Вестн. Рос. ун-та дружбы народов. Сер. Политология. — 2006. — № 1. — С. 68–80.

311. Нисневич Ю. А. Информационные основы административной реформы / Ю. А. Нисневич // НТИ. Сер. 1, Орг. и методика информ. работы. — 2002. — № 4. — С. 9–14.

312. Нисневич Ю. Л. Системно-методологические основы государственной информационной политики / Ю. Л. Нисневич // Науч.-техн. информ. Сер. 1. — 2001. — № 3. — С. 1–9.

313. Нисневич Ю. А. Информационная политика России / Ю.А.Нисневич. — М.: Мысль, 1998. — 350 с.

314. Нисневич Ю. А. Информационный фактор политической модернизации / Нисневич Ю. А // Вестник Московского университета. — Серия 12. — Политические науки. — М., 2001. — № 3. — С.91–101.

315. Нисневич Ю. А. Информация и власть / Ю. А.Нисневич. — М. : Мысль, 2000. — 175 с.

316. Ницше Ф. Сочинения. Т.1 / Ницше Ф. — М. : Мысль, 1991.— С.430.

317. Новая философская энциклопедия. В 4-х томах. / Рук. проекта В. С. Степин, Г.Ю. Семигин. — М. : Мысль, 2001. — С.42.

318. Новий словник іншомовних слів. Укладання і передмова О. М.Сліпушко. 20 000 слів. — К.: Аконіт, 2008. — С.740.

319. Новик И. Б. Метод моделирования в современной науке / И. Б. Новик, Н. М. Мамедов. — М. : Знание РСФСР, 1981. — 40 с.

320. Ноэль-Нойман Э. Общественное мнение: Открытие спирали молчания / Э. Ноэль-Нойман. — М., 1996.— С. 96.

321. О. В.Литвиненко. Інформаційний простір як чинник забезпечення національних інтересів України / О. В.Литвиненко, І. Ф.Бінько, В. М.Потіха. — К. : Київський університет ім. Т.Г.Шевченка. Інститут міжнародних відносин. — 1998. — 47с.

322. Оболенський О. Ю. Теорія системного підходу в державному управління / О. Ю. Оболенський // Вісник НАДУ. —1996. — № 3. — С. 151–158.

323. Одінцова Г. С. Теорія та історія державного управління: Навч. посіб / Г. С.Одінцова, В. Б.Дзюнджюк, Н. М.Мельтюхова. — К. : «Видавничий дім «Професіонал», 2008. — 288 с.

324. Окінавська хартія глобального інформаційного суспільства від 22. 07.2000 р. // Дипломат. вестн. — 2000. — № 8. — С. 51–56.

325. Олійник О. В. Державна інформаційна політика та інформаційна безпека України: політико-правові аспекти / Олійник О. В. // Право України. — 2005. — №5. — С. 108–111.

326. Ортега-и-Гассет Х. Восстание масс / Ортега-и-Гассет Х. — М., 2001. — С. 119.

327. Павлов А. Н. Информационные технологии управления / А. Н. Павлов. — М., 2001.— С. 68.

328. Палькина Т. Единое информационное пространство Здравоохранения /Т.Палькина. http://www.cnews.ru/reviews/free/national2006/articles/edin_info/ 19.12.2006.

329. Панарин А. Стратегическая нестабильность XXI века / Панарин А. // «Москва», № 4–12, 2002 г.

330. Парахонский Б. А. Язык культуры и генезис знания / Б. А. Парахонский — Киев : Наук. думка, 1988. — 212 с.

331. Петровський П. М. Інститут інформації як інфраструктурне підґрунтя комунікативної взаємодії держави та суспільства / П. М. Петровський, О. В. Радченко // Актуальні проблеми державного управління: Зб. наук. пр. Одеського регіонального інституту державного управління. — Одеса : Вид-во ОРІДУ НАДУ, 2011.— № 1 — С. 22 – 26.

332. Перепелиця Г. Асиметричні стратегії в гарантуванні міжнародної безпеки / Г. Перепелиця // Політика і час. — 2005. — № 7. — С. 64–76.

333. Петренко С. А. Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. — М. : ДМКпресс, 2006.— 235 с.

334. Петрик В. М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій / Петрик В. М., Остроухов В. В. та ін.: Навчальний посібник. — К. : Росава, 2006. — 208 с.

335. Петрова Е. В. Информационная политика территориальных органов управления в системе государственной информационной политики современной России [Текст]: автореф. канд. политических наук: спец. 23.00.02 (политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии) / Петрова Е. В. — 2004.— 20 с.

336. План действий // Всемирный Саммит по информационному обществу. — СПб., 2004. — С. 25–47.

337. План дій «Україна — Європейський Союз» : Європейська політика сусідства [Електронний ресурс] : схвал. Кабінетом Міністрів України 12.02.2005 р., схвал. Радою з питань співробітництва між Україною і

Європейським Союзом 21.02.2005 р. — Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_693. — Назва з екрана.

338. Платон. Государство // Платон. Филеб, Государство, Тимей, Критий. — М., 1999. — С. 140–144, 149–158.

339. Политическая энциклопедия. В 2-х томах./ Рук. проекта Г. Ю. Семигин. — М.: Мысль, 1999. — С. 461.

340. Политология: Энциклопедический словарь / Общ. ред. и сост. Ю. И.Аверьянов. — М., 1993. — С. 251–256.

341. Полякова Л. П. Державне управління інформаційно-освітнім середовищем інноваційних університетських комплексів: монографія / Л. П. Полякова; під. заг. ред. О. С. Поважного. — Донецьк: «Ноулідж» (донецьке відділення). 2010. — 351 с.

342. Пономаренко Г. О. Управління у сфері забезпечення внутрішньої безпеки держави: адміністративно-правові засади: [монографія] / Пономаренко Г. О. — Харків: Видавець ФО-П Вапнярчук Н.М., 2007. — 448 с.

343. Попов В. Д. Государственная информационная политика: состояние и проблемы формирования / В. Д. Попов // Массовые информационные процессы в современной России : очерки / Рос. акад. гос. службы при Президенте Рос. Федерации ; [отв. ред. А. В. Шевченко]. — М., 2002.

344. Попов В. Д. Информациология и информационная политика / В. Д. Попов ; Рос. акад. гос. службы при Президенте Рос. Федерации. — М. : Изд-во РАГС, 2001. — 116 с.

345. Попов В. Д. Информационная политика: Учебник / Под общ. Ред. В. Д. Попова. — М. : Изд-во РАГС, 2003. — 463 с.

346. Попов В. Д. Парадоксы в судьбе России (коммуникативный психоанализ власти и общества) / Попов В. Д. — М., 2005.— С. 85.

347. Попов В. Д. Тайны информационной политики: социокоммуникативный психоанализ информационных процессов. [Монография] / Попов В. Д. Изд. 2-е, доп. и переработ. М., 2006. — С.4.

348. Про електронний цифровий підпис.— Закон України від 22 трав. 2003 р. № 852 // Відом. Верховної Ради України. — 2003. — № 36. — Ст. 276.

349. Попов И. И. Информационная безопасность / Попов И. И., Партыка Т. Л. — М. : Форум, 2007.— С. 39.

350. Порядок надання інформаційних та інших послуг із використанням електронної інформаційної системи «Електронний Уряд» : затв. наказом Держ. ком. зв'язку та інформатизації України від 15 серп. 2003 р. № 149 // Офіц. вісн. України. — 2003. — № 48. — С. 310–320.

351. Поппер К.Р. Открытое общество и его враги. Т.1 / Поппер К. Р. — М. : Феникс, 1992. (Popper K. The Open Society and its Enemies, a.a.O., Kap. 5: Nature and Convention).

352. Постанова Верховної Ради України "Про Концепцію (основи державної політики) національної безпеки України" від 16 січня 1997 р. № 3/97 ВР // Голос України. — 1997. — 4 лютого. — С. 5.

353. Постанова Верховної Ради України «Про прийняття за основу проекту Закону України про Концепцію державної інформаційної політики» від 11 січня 2011 року [Електронний ресурс]. — Режим доступу: search.ligazakon.ua›l_doc2.nsf/link1/T113590.html

354. Постанова Кабінету Міністрів України від 3 серпня 2005 р. № 688 «Про затвердження Положення про Реєстр інформаційних, телекомунікаційних, та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» // Офіційний вісник України, 2005.— № 31. — том 2. — Ст. 1869.

355. Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» : постанова Кабінету Міністрів України від 24 лют. 2003 р. № 208 // Офіц. вісн. України. — 2003. — № 9. — С. 112–114.

356. Почепцов Г. Г. Інформаційна політика : навч. посіб. / Г. Г. Почепцов, С. А. Чукут. — К. : Знання, 2006. — 663 с.

357. Про затвердження Порядку акредитації центру сертифікації ключів : постанова Кабінету Міністрів України від 13 черв. 2004 р. № 903 // Офіц. вісн. України. — 2004. — № 28, т. 1. — С. 108–114.

358. Про затвердження Порядку обов'язкової передачі документованої інформації : постанова Кабінету Міністрів України від 28 жовт. 2004 р. № 1454 // Офіц. вісн. України. — 2004. — № 44. — С. 131–133.

359. Почепцов Г. Г. Теория коммуникации / Георгий Поцепцов. — М. : Рефл-бук, 2003. — 651 с.

360. Почепцов Г. Как «переключают» народы / Почепцов Г. — Киев, 1998.

361. Почепцов Г. Стратегические коммуникации в современном мире / Георгий Почепцов // PR-менеджер. — 2009. — № 4. — С. 3–11.

362. Почепцов Г. Г. Коммуникативные технологии XX века / Почепцов Г. — М., 2000.— С. 49.

363. Почепцов Г. Г. Національна безпека країн перехідного періоду: Навч. посіб / Почепцов Г. Г. — К., 1996. — 378 с.

364. Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади : указ Президента України від 1 серп. 2002 р. № 683 // Офіц. вісн. України. — 2002. — № 31. — С. 192–194.

365. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади : постанова Кабінету Міністрів України від 4 січ. 2002 р. № 3 // Офіц. вісн. України. — 2002. — № 2. — С. 234–238.

366. Про вдосконалення державного управління інформаційною сферою : указ Президента України від 16 верес. 1998 р. № 1033 // Офіц. вісн. України. — 1998. — № 38. — С. 3.

367. Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади: Указ Президента України від 14 липня 2000 р. // Урядовий кур'єр. — 2000. — № 128.

368. Про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України: Указ Президента України від 6 жовтня 2000 р. // Офіційний Вісник України. — 2000. — № 41.

369. Про заходи щодо забезпечення інформаційної безпеки держави: Указ Президента України від 18 вересня 2002 р. // Офіційний Вісник України. — 2002. — № 38. — Ст. 1771.

370. Про заходи щодо захисту інформаційних ресурсів держави: Указ Президента України від 10 квітня 2000 р. // Офіційний Вісник України. — 2000. — № 15.

371. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні : указ Президента України від 31 лип. 2000 р. № 928 // Офіц. вісн. України. — 2000. — № 31. — С. 11–13.

372. Про Концепцію (основи державної політики) національної безпеки України. Постанова Верховної Ради України від 18 липня 1995 р. № 532-95-п. (Із змінами, внесеними згідно з Постановою КМ N 1849 (1849-98-п) від 23.11.98). Відомості Верховної Ради. — 1997. — N10, ст.85.

373. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України: Указ Президента України від 22 січня 2002 р. // Офіційний Вісник України. — 2002. — № 4. — Ст. 132.

374. Про рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 31 жовтня 2001 року : указ Президента України від 6 груд. 2001 р. № 1193 // Офіц. вісн. України. — 2001. — № 50. — С. 28.

375. Про рішення Ради національної безпеки і оборони України від 19 липня 2001 р. „Про заходи щодо захисту національних інтересів у галузі

зв’язку та телекомунікацій: Указ Президента України від 23 серпня 2001 р. // Офіційний Вісник України. — 2001. — № 35. — Ст. 1622.

376. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року з питання „Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки”: Указ Президента України від 6 грудня 2001 р. // Офіційний Вісник України 2001. — № 50. — Ст. 2228.

377. Про удосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади: Указ Президента України від 14 липня 2000 р. // Урядовий кур’єр. — 2000. — 18 липня.

378. Про заходи щодо подальшого забезпечення відкритості у діяльності органів виконавчої влади : постанова Кабінету Міністрів України від 29 серп. 2002 р. № 1302 // Офіц. вісн. України. — 2002. — № 36. — С. 83–85).

379. Программа ЮНЕСКО «Информация для всех». Отчет 2004–2005 [Текст]: [перс англ.] / Л. В. Петрова; Российский комитет Программы ЮНЕСКО «Информация для всех». — М., 2006. — 165 с.

380. Проигрывает ли Украина в информационной войне на своей территории: Інтернет-ресурс: Режим доступу. — http://dialogs.org.ua/project_ua_full.php?m_id=9802.

381. Пугачев В. П. Технологии скрытого управления в современной российской политике / Пугачев В. П. // Вестник Московского университета. Серия 12. Политические науки. — 2003, № 3. — С. 66–102.

382. Пулим О. В. Актуальні проблеми забезпечення національної безпеки України у контексті розширення НАТО на схід / О. В. Пулим // Зб. наук. пр. / Військовий гуманітар. ін.-т Нац. академії оборони України. — К., 2000. — № 4. — С. 45–52.

383. Пушкарева Г. В. Политический менеджмент: Учебное пособие / Пушкарева Г. В. — М., 2002. — С. 14–27.

384. Рада Європи. Комітет міністрів. Рекомендація Rec (2002) 2 Про доступ до офіційних документів (Ухвалена Комітетом міністрів 21 лютого 2002 року на 784-му засіданні заступників міністрів).

385. Расторгуев С. П. Информационная война./ С. П. Расторгуев. — М.: Радио и связь, 1998. — 415 с.

386. Радченко О. В. Ідеї демократії як субстрат ціннісної системи українського суспільства: історичний екскурс / О.В. Радченко // Держава та регіони. Науково-виробничий журнал. — Запоріжжя, 2008. — № 3. — С. 166–171.

387. Результаты днепропетровского социологического исследования «информационное поле Днепропетровска». Інтернет-ресурс: Режим доступу. — http://most-dnepr.info/news/research/7880.htm.

388. Рейман Л. Д. Взаимодействие безопасностей / Л. Д. Рейман // Вестник связи International. — 2003. — № 4.

389. Растригин Л.А. Адаптация в сложных системах / Растригин Л.А. — Рига: Зинатне, 1981.— С. 23.

390. Рижих В. М. Державне управління науково-технічним прогресом: економічні аспекти / В. М. Рижих. — Х. : Прапор, 1998. — 398 с.

391. Руководящие принципы политики совершенствования государственной информации, являющейся общественным достоянием / подгот. Полом Ф. Улиром. — Париж : ЮНЕСКО, 2004. — 39 с.

392. Растригин Л. А. Современные принципы управления сложными объектами / Растригин Л. А. — М.: Сов. радио, 1980.— С. 88.

393. Семенюк Э. П. Социокультурная интеграция человечества и информатика / Э. П. Семенюк // НТИ. Сер. 1, Орг. и методика информ. работы. — 2009. — № 1. — С. 1–12.

394. Сендзюк М. А. Інформаційні системи в державному управлінні : навч. посіб. / М. А. Сендзюк. — К. : КНЕУ, 2004. — 339 с.

395. Синергетика. Философия. Культура. — М., 2001. — С. 4–9.

396. Системные основы государственной информационной политики // В кн.: Массовые информационные процессы в современной России. Очерки. Отв. ред. А.В. Шевченко. — М.: Изд-во РАГС, 2002.

397. Скаленко О. К. Інформація та інформаційні знання в глобальному інформаційному суспільстві / О. К. Скаленко, Г. О. Пархоменко, Б. В. Пархоменко // Наук.-техн. інформ. — 2005. — № 2. — С. 3–5.

398. Скопцов В.В. Социальный фрактал как фактор минимизации уровня неопределенности в социуме / Скопцов В.В. — [Электронный ресурс]. — Режим доступа : www .psyfactor.org

399. Сладкова О. Б. Манипулирование общественным сознанием в информационном обществе / О. Б. Сладкова // Обсерватория культуры. — 2006. — № 6. — С. 4–12.

400. Словарь русского языка: В 4 т. — Т. 3. — М.: Русский язык, 1981. — С. 261.

401. Смолян Г. Л. Проблемы обеспечения гарантий безопасности информационного общества / Г. Л. Смолян, А. А. Кононов // НТИ. Сер. 1, Орг. и методика информ. работы. — 2003. — № 8. — С. 13–18.

402. Сморгунов Л. В. Государственное управление и политика: Учеб. пособие / Под ред. Л.В. Сморгунова. — СПб. — 2002. — С. 124.

403. Соболев В. Информация и переходная инфраструктуры / Соболев В. // Бизнес. Информ. — 1999 — № 3–4. — С. 36.

404. Совершенствование деятельности органов государственной власти и местного самоуправления на основе использования информационных технологий [Электронный ресурс]. Ч. 2. Вып. 13. — 2002. — Режим доступа : http://www.microsoft.com/rus/government/newsletters/issue13. — Загл. с экрана.

405. Соловьев А. И. Политология: политическая теория, политические технологии: Учебник для студентов вузов / А.И. Соловьев. — М.— 2006.— С. 394, 395, 408, 409.

406. Сорокин К. Э. Дилеммы и казусы геополитики / Сорокин К. Э. — Режим доступа : http://www.politstudies.ru/fulltext/1995/1/2.htm

407. Соснін О. Важлива складова національної безпеки (проблеми захисту науково-технічної інформації) / О. Соснін // Вісн. НАН України [Електронний ресурс]. — 2002. — № 12. — Режим доступу до журн.: www.nbuv.gov.ua/artikles/vis-nanu/2002-12/4.html/. — Назва з екрана.

408. Социальная информациология: Словарь / Сост. Л. И. Мухамедова, Под общ.ред. В. Д. Попова. — М., 2006. — С.42.

409. Социологическая энциклопедия. В 2 т. Т. 1. — М. : Мысль, 2003. — 390 с.

410. Социологический энциклопедический словарь. — М., 1998. — С. 133.

411. Соціологічне опитування Центру Разумкова «На яке джерело Ви покладаєтеся найбільше в отриманні інформації про партії та блоки?». Інтернет-ресурс: Режим доступу.— http://razumkov.org.ua/ukr/poll.php?poll_id=225

412. Соціологічне опитування Центру Разумкова «Оцініть за п'ятибальною шкалою рівень свободи слова в Україні». Інтернет-ресурс:Режим доступу. – http://razumkov.org.ua/ukr/poll.php?poll_id=564

413. Соціологічне опитування Центру Разумкова «Чи довіряєте Ви західним ЗМІ?» (динаміка, 2000-2011). Інтернет-ресурс: Режим доступу. — http://razumkov.org.ua/ukr/poll.php?poll_id=85

414. Соціологічне опитування Центру Разумкова «Чи довіряєте Ви ЗМІ Росії?» (динаміка, 2000-2011). Інтернет-ресурс: Режим доступу. — http://razumkov.org.ua/ukr/poll.php?poll_id=86

415. Соціологічне опитування Центру Разумкова «Чи можуть бути обмежені свобода слова і свобода засобів масової інформації?». Інтернет-ресурс: Режим доступу. – http://razumkov.org.ua/ukr/poll.php?poll_id=359

416. Соціологічне опитування Центру Разумкова: «З яких джерел Ви в основному отримуєте інформацію про партії та блоки?». Інтернет-ресурс: Режим доступу. – http://razumkov.org.ua/ukr/poll.php?poll_id=224

417. Соціологічне опитування Центру Разумкова: «Чи довіряєте Ви ЗМІ

України?» (динаміка, 2000-2011). Інтернет-ресурс: Режим доступу. — http://razumkov.org.ua/ukr/poll.php?poll_id=87

418. Соціологічне опитування Центру Разумкова: «Чи заважають незалежності України наступні фактори?» Інтернет-ресурс: Режим доступу. — http://razumkov.org.ua/ukr/poll.php?poll_id=591

419. Соціологічне опитування Центру Разумкова: «Чи можна в інтересах охорони моральності населення заборонити до показу по телебаченню публіцистичну або інформаційну передачу?» Інтернет-ресурс: Режим доступу. – http://razumkov.org.ua/ukr/poll.php?poll_id=463

420. Соціологічне опитування Центру Разумкова: «Чи можна в інтересах охорони моральності населення заборонити до показу по телебаченню та в кінотеатрах фільм?». Інтернет-ресурс: Режим доступу. — http://razumkov.org.ua/ukr/poll.php?poll_id=462

421. Соціологічне опитування Центру Разумкова: «Чи можна в інтересах охорони моральності населення обмежити громадянину право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб?» Інтернет-ресурс: Режим доступу. — http://razumkov.org.ua/ukr/poll.php?poll_id=468

422. Старіш О. Г. Інформаційна політика держави в контексті глобалізації: автореф. дис. на здобуття наук. ступеня доктора політичних наук: спец. 23.00.03 «Політична культура та ідеологія» / Старіш О. Г. — Київ. — 2008.— 40 с.

423. Старіш О. Г. Інформаційні процеси в структурі світових комунікаційних систем / О. Г. Старіш, А. А. Чічановський. — К. : Грамота, 2010. — 568 с.

424. Степанов В. Ю. Сучасний інформаційний простір: особливості та тенденції розвитку: [Текст]: монографія / В. Ю. Степанов; — Харків : Вид-во «С. А. М.», 2010. — 280 с.

425. Степанов В. Ю. Концептуальні засади формування та розвитку інформаційного успільства: державно-управлінський аспект [Текст]:

монографія / В. Ю. Степанов. — Х. : Вид-во «С.А.М.», 2010. — 416 с.

426. Степанов В. Ю. Державна інформаційна політика: проблеми та перспективи: [Текст.]: монографія / В. Ю. Степанов; — Харків : Вид-во «С. А. М.», 2011. — 548 с.

427. Степанов В. Ю. Управлінські рішення в органах державної влади [Текст]: монографія / А. О. Дєгтяр, В. Ю. Степанов, С. В. Тарабан ; за заг. ред. А. О. Дєгтяра. — Х. : Вид-во «С.А.М.», 2010. — 275 с.

428. Степанов В. Ю. Філософська концепція еволюції постіндустріального суспільства [Текст] / В. Ю. Степанов // Теорія та практика державного управління : [зб. наук. пр.] / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2009. — Вип. 4. — С. 68–78.

429. Степанов В. Ю. Інформація як суб'єкт відображення соціальної системи [Текст] / В. Ю. Степанов // Економіка та держава. — 2009. — № 12. — С. 51–53.

430. Степанов В. Ю. Концептуальні засади становлення та розвитку інформаційного суспільства [Текст] / В. Ю. Степанов // Теорія та практика державного управління : [зб. наук. пр.] / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2009. — Вип. 3. — С. 256–261.

431. Степанов В. Ю. Моделювання інформаційно-комунікативного простору в сучасному суспільстві [Текст] / В. Ю. Степанов // Державне будівництво [Електронне видання] — 2009.— № 2. — Режим доступу до журн. : http: // www.kbuapa.kharkov.ua

432. Степанов В. Ю. Інформаційний простір: соціально-економічний аспект [Текст] / В. Ю. Степанов // Інвестиції: практика та досвід. — 2009. — № 21. — С. 67–69.

433. Степанов В. Ю. Державне управління в інформаційному просторі [Текст] / В. Ю. Степанов // Держава та регіони. Сер. Держ. упр. — 2009. — № 4. — С. 83–87.

434. Степанов В. Ю. Концепція інформаційного забезпечення управлінських рішень [Текст] / В. Ю. Степанов // Ефективність державного

управління : зб. наук. пр. / Львів. регіон. ін-т держ. упр. Нац. акад. держ. упр. при Президентові України. — Л., 2009. — Вип. 18/19. — С. 420−425.

435. Степанов В. Ю. Державна інформаційна політика: регулювання міжпартійних конфліктів [Текст] / В. Ю. Степанов // Зб. наук. пр. Донец. держ. ун-ту упр. Сер. Держ. упр. / М-во освіти і науки України. — Донецьк, 2009. — Т. 10. — Вип. 144 : Державне управління регіонами і підприємствами. — С. 201–208.

436. Степанов В. Ю. Державне управління інформаційними ресурсами [Текст] / В. Ю. Степанов // Зб. наук. пр. Донец. держ. ун-ту упр. Сер. Держ. упр. / М-во освіти і науки України. — Донецьк, 2009. — Т. 10, вип. 132 : Соціальний менеджмент і управління інформаційними процесами. — С. 448–456.

437. Степанов В. Ю. Інформаційні технології в менеджменті: концептуальний аспект [Текст] / В. Ю. Степанов // Зб. наук. пр. Донец. держ. ун-ту упр. Сер. Держ. упр. / М-во освіти і науки України. — Донецьк, 2009. — Т. 10. — Вип. 142 : Державне управління регіонами і підприємствами. — С. 200–207.

438. Степанов В. Ю. Електронний уряд: проблеми реалізації [Текст] / В. Ю. Степанов // Актуальні проблеми державного управління : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2009. — № 2. — С. 81–86.

439. Степанов В. Ю. Електронна держава як атрибут державної інформаційної політики [Текст] / В. Ю. Степанов // Інвестиції: практика та досвід. — 2010. — № 3. — С. 76–78.

440. Степанов В. Ю. Вплив інформаційного простору на сучасне суспільство [Текст] / В. Ю. Степанов // Теорія та практика державного управління : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2010. — Вип. 2. — С. 24−30.

441. Степанов В. Ю. Концептуальні аспекти управління в сучасному інформаційному просторі [Текст] / В. Ю. Степанов // Теорія та практика

державного управління : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2010. — Вип. 1. — С. 29–34.

442. Степанов В. Ю. Інформаційна політика: концептуальні засади формування та розвитку [Текст] / В. Ю. Степанов // Теорія та практика державного управління : [зб. наук. пр.] / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2010. — Вип. 3. — С. 13–17.

443. Степанов В. Ю. Механізми формування та реалізації державної інформаційної політики в сучасних умовах [Текст] / В. Ю. Степанов // Держава та регіони. — 2010. — № 2. — С. 122–126.

444. Степанов В. Ю. Державна інформаційна політика в умовах розвитку суспільства [Текст] / В. Ю. Степанов // Інвестиції: практика та досвід. — 2010. — № 5. — С. 78–80.

445. Степанов В. Ю. Державна інформаційна політика: концептуальні напрями розвитку на сучасному етапі [Текст] / В. Ю. Степанов // Держава та регіони. Сер. Держ. упр. — 2010. — № 1. — С. 114–118.

446. Степанов В. Ю. Інтелектуальний менеджмент у контексті управлінської діяльності [Текст] / Степанов В. Ю. // Менеджер : вісн. Донец. держ. ун-ту упр. — 2010. — № 2. — С. 141–145.

447. Степанов В. Ю. Інформаційна культура менеджера в менеджменті: [Текст] / В. Ю. Степанов // Зб. наук. пр. Донец. держ. ун-ту упр. Сер. Держ. упр. / М-во освіти і науки України. — Донецьк, — 2010. — Том 11. — Вип. 174 : Державне управління регіонами і підприємствами. — С. 26–34.

448. Степанов В. Ю. Інформаційна політика: маніпулятивні технології у суспільстві [Текст] / В. Ю. Степанов // Економіка та держава. — 2010. — № 4. — С. 129–131.

449. Степанов В. Ю. Державна інформаційна політика у сфері інформаційного протиборства: теоретико-методологічний аспект [Текст] / В. Ю. Степанов // Актуальні проблеми державного управління : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2010. — № 1. — С. 128–135.

450. Степанов В. Ю. Державна інформаційна політика: концепція інформаційної безпеки [Текст] / В. Ю. Степанов // Держава та регіони. Сер. Державне управління. — 2010. — № 4. — С. 86–91.

451. Степанов В. Ю. Інформаційний менеджмент як атрибут управлінської діяльності та інформаційної політики [Текст] / В. Ю. Степанов // Менеджер : вісн. Донец. держ. ун-ту упр. — 2010. — № 3. — С. 227–231.

452. Степанов В. Ю. Комунікаційний аспект у системі управління [Текст] / В. Ю. Степанов // Економіка та держава. — 2010. — № 8. — С. 135–137.

453. Степанов В. Ю. Комунікація в політичній системі суспільства: державно-управлінський аспект [Текст] / В. Ю. Степанов // Теорія та практика державного управління : [зб. наук. пр.] / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2010. — Вип. 4. — С. 53–58.

454. Степанов В. Ю. Теоретико-методологічний аспект політичної комунікації в системі державного управління [Текст] / В. Ю. Степанов // Інвестиції: практика та досвід. — 2010. — № 12. — С. 73–75.

455. Степанов В. Ю. Сучасна політика органу влади: комунікативний аспект [Текст] / В. Ю. Степанов // Актуальні проблеми державного управління : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2010. — № 2. — С. 299–305.

456. Степанов В. Ю. Сучасні інформаційні технології в державному управлінні [Текст] / В. Ю. Степанов // Економіка та держава. — 2010. — № 9. — С. 101–103.

457. Степанов В. Ю. Управлінська функція інформації у державному управлінні [Текст] / В. Ю. Степанов // Ефективність державного управління : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Львів. регіон. ін-т держ. упр. — Л., 2010. — Вип. 22. — С. 300–306.

458. Степанов В. Ю. Державна інформаційна політика: мета та теоретичні засади реалізації [Текст] / В. Ю. Степанов // Держава та регіони. Сер. Держ. упр. — 2011. — № 2. — С. 91–96.

459. Степанов В. Ю. Інформаційна політика як інструмент сучасного державного управління [Текст] / В. Ю. Степанов // Держава та регіони. Сер. Держ. упр. — 2011. — № 1. — С. 83–87.

460. Степанов В. Ю. Державна інформаційна політика в сучасному політичному просторі [Текст] / В. Ю. Степанов // Інвестиції: практика та досвід. — 2011. — № 3. — С. 76–78.

461. Степанов В. Ю. Державна інформаційна політика як інструмент забезпечення єдиного інформаційного простору [Текст] / В. Ю. Степанов // Інвестиції: практика та досвід. — 2011. — № 4. — С. 78–81.

462. Степанов В. Ю. Концептуальні засади реалізації державної інформаційної політики [Текст] / В. Ю. Степанов // Теорія та практика державного управління : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2011. — Вип. 1. — С. 91–97.

463. Степанов В. Ю. Концептуальні напрями розвитку державної інформаційної політики на сучасному етапі [Текст] / В. Ю. Степанов // Державне управління та місцеве самоврядування : тези X Міжнар. наук. конгресу, 26 берез. 2010 р. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. — Х., 2010. — С. 28–29.

464. Степанов В. Ю. Державне управління: економічний аспект [Текст] / В. Ю. Степанов // Науково-практичні аспекти оптимізації управлінської діяльності органів державної влади та місцевого самоврядування : тези доп. Всеукр. наук.-практ. конф., 3 груд. 2010 р. / Класич. приват. ун-т, Ін-т держ. та муніцип. упр. — Запоріжжя, 2010. — С. 206–207.

465. Степанов В. Ю. Електронна демократія як тенденція розвитку громадянського суспільства [Текст] / В. Ю. Степанов // Управління розвитком : Всеукр. наук.-практ. конф. «Актуальні проблеми державного управління та державної служби в умовах постіндустріальної економіки», 26 лют. 2010 р. : зб. наук. робіт / Харк. нац. екон. ун-т. — Х., 2010. — № 8. — С. 35–37.

466. Степанов В. Ю. Перспективи розвитку електронного суспільства [Текст] / В. Ю. Степанов // Культура та інформаційне суспільство XXI століття.

У 2 ч. : матеріали всеукр. наук.-теорет. конф. молодих учених, 22–23 квіт. 2010 р. / М-во культури і туризму України, Харк. держ. акад. культури, Акад. мистец. України, Ін-т культурології. — Х., 2010. — Ч. 2. — С. 152.

467. Степанов В. Ю. Інформаційна політика держави та мас-медійна культура суспільства [Текст] / В. Ю. Степанов // Культурология та соціальні комунікації: інноваційні стратегії розвитку : матеріали міжнар. наук. конф., Харків, 18–19 листоп. 2010 р. / Харк. держ. акад. культури ; [ред. кол. В. М. Шейко та ін.]. — Х. : ХДАК, 2010. — 296 с.

468. Степанов В. Ю. Управлінська концепція в організації соціального підприємництва [Текст] / В. Ю. Степанов // Державне регулювання соціального підприємництва та соціально відповідального бізнесу : матеріали II Міжнар. наук.-практ. конф., 25 листоп. 2010 р. / Харк. облдержадмін. [та ін.]. — Х., 2010. — С. 103–105.

469. Степанов В. Ю. Управлінська функція інформації місцевого самоврядування [Текст] / В. Ю. Степанов // Державна політика щодо місцевого самоврядування: стан, проблеми та перспективи : [1 Всеукр. наук.-практ. конф., 7-9 жовт. 2010 р., Херсон] : зб. матеріалів конф. / Голов. упр. держ. служби України [та ін.]. — Херсон, 2010. — С. 38–39.

470. Степанов В. Ю. Управлінський аспект у вдосконаленні маркетингу [Текст] / В. Ю. Степанов // Управлінські аспекти підвищення національної конкурентоспроможності : матеріали IV міжнар. наук.-практ. конф., 21-23 жовт. 2010 р. / Самар. ін-т бізнесу та упр., Крим. ін-т бізнесу, Консалтингово-конфліктол. центр, Центр розвитку освіти, науки та інновацій. — Ялта, 2010. — С. 169–172.

471. Степанов В. Ю. Сучасне інформаційне суспільство та освіта: концептуальний аспект [Текст] / В. Ю. Степанов // Українська культура та ментальність: самобутність в умовах глобалізації / Матеріали III Всеукраїнської науково-практичної конференції 28–30 січня 2011 р. — Сімферополь: ЦРОНІ, 2011. — 116 с.

472. Степанов В. Ю. Реалізація державної інформаціонної політики: методологічний аспект [Текст] / В. Ю. Степанов // Державне управління та місцеве самоврядування : тези XI Міжнар. наук. Конгресу, 24 березня 2011 р. — Х. : Вид-во ХарРІНАДУ «Магістр», 2011. — 442 с.

473. Степанов В. Ю. Управлінська функція інформації на підприємствах [Текст] / Степанов В. Ю. // [II Міжнар. наук.-практ. конф., 17 лютого 2011 р., Донецьк] : Зб. наук. пр. Донец. держ. ун-ту упр. Сер. Держ. упр. / М-во освіти і науки України. — Донецьк, 2011. — С. 22–23.

474. Степанов В. Ю. Інформаційна безпека України в контексті інформаційної політики держави [Текст] / В. Ю. Степанов // Проблеми та перспективи формування гуманітарної політики в Україні / Матеріали круглого столу 25 лютого 2011 р. Відп. ред. В.В.Трофімова. — Сімферополь: ЦРОНІ, 2010. — 91 с.

475. Степанов В. Ю. Менеджмент інформаційних технологій [Текст] / В. Ю. Степанов // Вісн. Харк. держ. акад. культури : зб. наук. пр. : до 80-річчя Харк. держ. акад. культури. — Х., 2009. — Вип. 28. — С. 52–60.

476. Степанов В. Ю. Інформаційна культура сучасного інформаційного суспільства [Текст] / В. Ю. Степанов // Вісн. Харк. держ. акад. культури : зб. наук. пр. : до 80-річчя Харк. держ. акад. культури. — Х., 2009. — Вип. 27. — С. 91–97.

477. Степанов В. Ю. Інформаційно-комунікативний маркетинг як соціальна технологія [Текст] / В. Ю. Степанов // Вестн. Нац. техн. ун-та «ХПИ» : сб. науч. тр. — Харьков, 2009. — № 35-1 : Технический прогресс и эффективность производства : темат. вып. — С. 18–26.

478. Степанов В. Ю. Менеджмент у сфері культури [Текст] / В. Ю. Степанов // Культура України : зб. наук. пр. : до 80-річчя Харк. держ. акад. культури / М-во культури і туризму України, Харк. держ. акад. культури, [Акад. мистец. України, Ін-т культурології] ; за заг. ред. В. М. Шейка. — Х., 2009. — Вип. 27. — С. 14–20.

479. Степанов В. Ю. Культурологічний аспект інформаційного суспільства [Текст] / В. Ю. Степанов // Культура України : зб. наук. пр. / М-во культури і туризму України, Харк. держ. акад. культури, [Акад. мистец. України, Ін-т культурології]. — Х., 2009. — Вип. 28. — С. 49–58.

480. Степанов В. Ю. Інформаційне суспільство: концептуальний аспект філософії [Текст] / В. Ю. Степанов // Культура України : зб. наук. пр. / М-во культури і туризму України, Харк. держ. акад. культури, [Акад. мистец. України, Ін-т культурології] ; за заг. ред. В. М. Шейка. — Х., 2010. — Вип. 31. — С. 98–106.

481. Степанов В. Ю. Інформаційне суспільство: культура особистості [Текст] / В. Ю. Степанов // Культура України : зб. наук. пр. / М-во культури і туризму України, Харк. держ. акад. культури, [Акад. мистец. України, Ін-т культурології] ; за заг. ред. В. М. Шейка. — Х., 2010. — Вип. 30. — С. 78–85.

482. Степанов В. Ю. Інформаційні технології як засіб забезпечення комунікацій у державному управлінні [Текст] / В. Ю. Степанов // Вісн. Харк. держ. акад. культури : зб. наук. пр. — Х., 2010. — Вип. 31. — С. 88–97.

483. Степанов В. Ю. Інформаційно-комунікаційні технології в сучасній освіті [Текст] / В. Ю. Степанов // Вісн. Харк. держ. акад. культури : зб. наук. пр. — Х., 2010. — Вип. 30. — С. 173–179.

484. Степанов В. Ю. Концептуальний аспект медіакультури в контексті інформаційної політики держави [Текст] / В. Ю. Степанов // Культура України : зб. наук. пр. / М-во культури і туризму України, Харк. держ. акад. культури, [Акад. мистец. України, Ін-т культурології] ; за заг. ред. В. М. Шейка. — Х., 2010. — Вип. 32. — С. 102–110.

485. Степанов В. Ю. Масова культура сучасного суспільства [Текст] / В. Ю. Степанов // Культура України : зб. наук. пр. / М-во культури і туризму України, Харк. держ. акад. культури, [Акад. мистец. України, Ін-т культурології]. — Х., 2010. — Вип. 29. — С. 30–38.

486. Степанов В. Ю. Менеджмент знань як аспект управлінської діяльності в інформаційному суспільстві [Текст] / В. Ю. Степанов // Вісн. Харк. держ. акад. культури : зб. наук. пр. — Х., 2010. — Вип. 29. — С. 58–65.

487. Степанов В. Ю. Соціокультурна концепція еволюції інформаційного середовища [Текст] / В. Ю. Степанов // Культура України : зб. наук. пр. / М-во культури і туризму України, Харк. держ. акад. культури, [Акад. мистец. України, Ін-т культурології]. — Х., 2011. — Вип. 33. — С. 61–67.

488. Степанов В. Ю. Держава як основний суб'єкт системи масових політичних комунікацій [Текст] / В. Ю. Степанов // Вісн. Харк. держ. акад. культури : зб. наук. пр. — Х., 2011. — Вип. 32. — С. 94–101.

489. Степанчиков С. Телекомунікаційний ринок охолоджується / С. Степанчиков // Дзеркало тижня. — 2008. — № 2 (681) 19 січня 2008 р. — С. 9.

490. Стенограма «круглого столу» «Інформаційна відкритість державної влади як запорука ефективної політики» 21.01.2005 р. — Режим доступу: www.ucipr.kiev.ua

491. Сіленко А. Соціально-політичні наслідки інформаційної революції / Алла Сіленко // Політ. менеджмент, 2005.— № 5.— С. 61–74.

492. Сляднева Н. А. Информационно-аналитическая деятельность: проблемы и перспективы / Н. А. Сляднева // Информационные ресурсы страны. — 2001. — № 2. — С. 14.

493. Сморгунов Л. В. Электронное правительство: этапы становления и равнение опыта / Л. В. Сморгунов // Технологии информационного общества — Интернет и современное общество: труды V Всероссийской объединенной конференции (Санкт-Петербург, 25–29 ноября 2002г.). СПб.: Изд-во С.-Петерб. ун-та, 2002. — С. 302–305.

494. Смирнова В. В. Интеллектуальные системы управления в условиях глобализации информационного пространства / В. В. Смирнова // Наукові праці

Донецького національного технічного університету. Серія: економічна. Вип. 84. — Донецьк: ДонНТУ, 2004. — С. 178–183.

495. Степин В. С. Теоретическое знание / В. С. Степин — М., 2000.— С. 29.

496. Степин В. С. Саморазвивающиеся системы и постнеклассическая рациональность / В. С. Степин // Вопросы философии. 2003. — № 8.

497. Столяров Ю. Н. Онтологический статус документа и его практическое значение для библиотек / Ю. Н. Столяров // Библиотековедение. — 1999. — № 4. — С. 50–59.

498. Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики / Т. Стоуньер. — М., 1986. — С. 395–396.

499. Стюгин М. Оценка безопасности и информационного управления Российской Федерации / Стюгин М. — 2006.

500. Тавокин Е. П. Информация как научная категория / Е. П. Тавокин // Социс. — 2006. — № 11. — С. 3–10.

501. Тавокин Е. П. Системные основы государственной информационной политики / Е. П. Тавокин // В кн.: Массовые информационные процессы в современной России. Очерки. Отв. ред. А.В. Шевченко. — М.: РАГС, 2002.

502. Таіров А. Інформаційне забезпечення функціонування органів державної влади: автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр.: 25.00.02 «Механізми державного управління» [Електронний ресурс] / А. І. Таіров, К, 2010.— 20 с.

503. Тапскотт Д. Электронно-цифровое общество: Плюсы и минусы эпохи сетевого интеллекта / Тапскотт Д. — М.– К., 1999. — С. 64.

504. Тихонравов Ю.В. Геополитика: Учебное пособие / Тихонравов Ю. В. — М.: ИНФРА-М, 2000 (Серия «Высшее образование»).

505. Токовенко В. В. Політичне керівництво і державне управління: проблеми взаємовідносин та оптимізації взаємодії: [Монографія] / В. В.Токовенко. — К.: Вид-во УАДУ, 2001.— 256 с.

506. Тоффлер Е. Нова парадигма влади: знання, багатство й сила / Елвін Тоффлер , пер. з англ. Н. Бордукової. — К. : Акта, 2003. — 685 с.

507. Тоффлер Э. Метаморфозы власти / Э. Тоффлер. — М., 2004. — С. 451.

508. Тоффлер Э. Третья волна / Элвин Тоффлер, пер. с англ. К. Ю. Бурмистрова. — М. : АСТ, 2009. — 795 с.

509. Тоффлер Э. Шок будущего / Э. Тоффлер. — М. : Логос, 2000. — 328 с.

510. Трач Ю. Інтернет як організаційно-технологічна основа становлення інформаційного суспільства / Юлія Трач // Вісн. Кн. палати. — 2007. — № 4. — С. 34–36.

511. Тронь В. П. Стратегія прориву: [Монографія] / Тронь В. П.— К.: Вид-во УАДУ, 1996. — 344 с.

512. Турен А. Возвращение человека действующего = Le retour de L'acteur : очерк социологии / Ален Турен ; [пер. с фр. Е. А. Самарской]. —М. : Науч. мир, 1998. — 203 с.

513. Турчинов А. И. Профессионализация и кадровая политика: проблемы развития теории и практики / Турчинов А. И. — М.: Московский псхолого-социальный институт, Флинт, 1998.— С. 92.

514. Удовик С. Л. Глобализация: семиотические подходы / Удовик С. Л. — М. — Киев, 2002.— С. 145.

515. Указ Президента України “Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади” (14.07.2000 р.);

516. Указ Президента України “Про заходи щодо захисту національних інтересів у галузі зв’язку та телекомунікацій” (23.08.2001р.)

517. Указ Президента України «Про деякі заходи щодо захисту держави в інформаційній сфері» (22.04.98 р.);

518. Указ Президента України «Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, дальшого утвердження

свободи слова в Україні» (09.12.2000 р.); «Про рішення Ради національної безпеки і оборони України» від 19 липня 2001 року

519. Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі» (31.07.2000 р.);

520. Указ Президента України № 1033 / 98 від 16 вересня 1998 року «Про вдосконалення державного управління інформаційною сферою» // Єдиний державний реєстр нормативно-правових актів, № 6041 / 1998.

521. Указ Президента України № 1276 / 2005 від 15 вересня 2005 року «Про забезпечення участі громадськості у формуванні та реалізації державної політики» // Офіційний вісник України, 2005. — № 38. — ст. 2363.

522. Указ Президента України № 1338 / 2005 від 26 вересня 2005 року «Про вдосконалення державного управління в інформаційній сфері» // Офіційний вісник України, 2005. — № 39. — ст. 2455.

523. Указ Президента України № 325 від 17 травня 2001 року «Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади» // Урядовий кур`єр, 2001. – № 88 від 22. 15. 2001 р.

524. Указ Президента України № 377/ 2008 від 23 квітня 2008 року. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладрні заходи щодо забезпечення інформаційної безпеки України» // Відомості Верховної Ради, 2008.— №4. — ст. 102.

525. Указ Президента України № 514 / 2009 від 8 липня 2009 року «Про Доктрину інформаційної безпеки України».

526. Уманський Ю. Інформація як основа інформаційно-аналітичного забезпечення державного управління / Ю. Уманський // Економіка і держава. — 2007. — № 11. — С. 87–88.

527. Урсул А. Д. Глобализация, устойчивое развитие, ноосферогенез: информационные аспекты / А. Д. Урсул, Т. А. Урсул // НТИ. Сер. 1, Орг. и методика информ. работы. — 2005. — № 4. — С. 1–15.

528. Урсул А. Д. Информационный вектор универсальной эволюции / А. Д. Урсул, Т. А. Урсул // НТИ. Сер. 1, Орг. и методика информ. работы. — 2005. — № 9. — С. 10–11.

529. Урсул А. Д. Универсальный эволюционизм: информационно-синергетический подход и общенаучные принципы / А. Д. Урсул, Т. А. Урсул // Соц.-гуманитар. знания. — 2006. — № 6. — С. 278–294.

530. Урсул Т. А. Концепция универсальной эволюции: социоприродное измерение / Т. А. Урсул // Соц.-гуманитар. знания. — 2006. — № 1. — С. 301–314.

531. Учение В. И. Вернадского о переходе биосферы в ноосферу, его философское и общенаучное значение / Учение В. И. — Т. 1 : сб. ст. — М. : Филос. о-во СССР, 1990. — 236 с.

532. Уэбстер Ф. Теории информационного общества / Ф. Уэбстер. — М. : Аспект Пресс, 2004. — 400 с.

533. Федотова Л. Н. Анализ содержания — социологический метод изучения средств массовой коммуникации : учеб. пособие / Л. Н. Федотова. — 2-е изд., испр. и доп. — М. : Науч. мир, 2001. — 212 с.

534. Философский энциклопедический словарь. М.: ИНФРА-М, 1998. — С. 185-186.

535. Фрейд 3. Массовая психология и анализ человеческого «Я» / 3. Фрейд // Избранное. Лондон, Т.1, 1969. — С. 116.

536. Фукуяма Ф. Конец истории./ Ф. Фукуяма // Вопросы философии, 1990. — С. 24.

537. Хабермас Ю. Будущее человеческой природы: на пути к либеральной евгенике? /Ю. Хабермас ; пер. с нем. М. Л. Хорькова. — М. : Весь Мир, 2002. — 144 с.

538. Хабермас Ю. Вовлечение другого: очерки политической теории / Ю. Хабермас ; пер. с нем. Ю. С Медведева ; под ред. Д. А. Скляднева. — М. : Наука, 2001. — 417 с.

539. Хабермас Ю. Когда мы должны быть толерантными? О конкуренции видений мира, ценностей и теорий / Ю. Хабермас ; пер. с нем. А. А. Зотова // Социс. — 2006. — № 1. — С. 45–53.

540. Хабермас Ю. Моральное сознание и коммуникативное действие : пер. с нем. / Юрген Хабермас. — СПб. : Наука, 2000. — 377 с. — (Серия «Слово о сущем»).

541. Хабермас Ю. Спор о прошлом и будущем международного права. Переход от национального к постнациональному контексту / Юрген Хабермас // Вопр. философии. — 2004. — № 3. — С. 12–18.

542. Хабермас Ю. Философский дискурс о модерне : [сб. лекций] / Юрген Хабермас ; пер. с нем. [М. М. Беляева и др.]. — М. : Весь мир, 2003. — 414 с.

543. Хакен Г. Информация и самоорганизация / Хакен Г. — М., 2001.— С.12.

544. Хантингтон С. Ф. Политический порядок в меняющихся обществах / Сэмюэл Хантингтон ; пер. с англ. В. Р. Рокитянского. — М. : Прогресс-Традиция, 2004. — 480 с.

545. Харченко Л. С. Інформаційна безпека України : глосарій / Л. С. Марченко, В. А. Ліпкан, О. В. Логінов. — К. : Текст, 2004. — 136 с.

546. Хилько О. Л. Актуальні проблеми розвитку безпекової та оборонної політики ЄС : сборник / О. Л. Хилько // Нова парадигма : Філософія. Соціологія. Політологія: Журнал наукових праць / НПУ ім. М. П. Драгоманова, Творче об'єднання "Нова парадигма". — Київ : НПУ, 2007. — Вип. 67. — С. 118–127.

547. Цвєтков В. В. Державне управління: основні фактори ефективності (політико-правовий аспект) / В. В. Цвєтков. — Х. : Право, 1996. — 164 с.

548. Цегольник П. Оптимізація процесу підготовки фахівців з державного управління на основі апарату моделювання / П. Цегольник // Вісник УАДУ. — 2000. — № 1. — С. 325–331.

549. Цимбалюк В. С. Інформаційне право (основи теорії і практики). [Монографія] / Цимбалюк В. С. — К : «Освіта україни», 2010. — 388 с.

550. Цурюпа М. В. Безпека міжнародна / М. В. Цурюпа, В. О. Храмов // Міжнародна поліцейська енциклопедія: У 10 Т. / відп. ред. Ю. І. Римаренко, Я. Ю. Кондратьєв, В. Я. Тацій, Ю. С. Шемшученко. — К. : Концерн „Видавничий дім „Ін юре", 2003. — Т. 1. — С. 50.

551. Цымбал В. И. О концепции информационной войны / В. И. Цымбал // Информационный сборник «Безопасность». — 1995. — № 9.

552. Черниш Н. Політичні трансформації в Україні у 90-х роках / Н. Черниш // Польща — Німеччина — Україна в Європі. — Жешув, 1998. — С. 45–58.

553. Чернюк Л. Г. Розміщення продуктивних сил України : навч. посіб. / Л. Г. Чернюк, Д. В. Клиновий. — К. : ЦУЛ, 2002. — 440 с.

554. Чуйко З. Д. Процеси глобалізації і проблеми національної безпеки / З. Д. Чуйко // Вісн. Луган. держ. ун-ту внутр. справ. — 2007. — Вип. 1. — С. 38–47.

555. Чукут С. А. Державна культурна політика України в контексті сучасного світового досвіду: основні напрямки і тенденції розвитку / С. А. Чукут // Вісн. Держ. акад. кер. кадрів культури і мистец. — 2001. — № 1. — С. 12–19.

556. Шагинян Г. А. Лингвистические аспекты освещения контртеррористических операций в государственных электронных СМИ / Г. А. Шагинян // Экологический вестник научных центров черноморского экономического сотрудничества. Дискурсивное пространство: эволюция и интерпретации. Краснодар, 2006. Приложение № 2. — С. 163–165

557. Шагинян Г. А. Проблема социальной ответственности СМИ в условиях борьбы с терроризмом / Г. А. Шагинян // Социальное партнерство как способ достижения гражданского согласия и социального мира, обеспечения стабильности общества: Материалы международной научно-практической

конференции (март 2006 г. Краснодар). Краснодар: Изд-во Кубан. гос. ун-та, 2006. — С. 165–166.

558. Швець М. Інформаційне законодавство України: концептуальні основи формування / М. Швець // Право України. — 2001. — № 7. — С. 88–94.

559. Швець М. Нова технологія законотворення : [інформ.-пошукові системи в Україні] / М. Швець // Право України. — 2003. — № 3. — С. 3–8.

560. Шевченко А. В. Информационная устойчивость политической системы / Шевченко А. В. — М., 2004.

561. Шейко В. Інформаційна цивілізація: проблеми становлення та розвитку / В. Шейко // Вісн. Кн. палати. — 2000. — № 6. — С. 11–14.

562. Шейко В. М. Формування інформаційного простору та зовнішньої культурної політики України в роки незалежності / В. М. Шейко // Вісн. Харк. держ. акад. культури : зб. наук. пр. — Х., 2010. — Вип. 29. — С. 4–17.

563. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. — М. : Изд-во иностр. лит., 1963. — 830 с.

564. Шехтман Л. И. Системы телекоммуникаций: проблемы и перспективы / Шехтман Л. И. — М.: Радио и связь, 1998.— №4.

565. Шрейдер Ю. А. Логика знаковых систем : элементы семиотики / Ю. А. Шрейдер. — Изд. 2-е. — М. : УРСС, 2010. — 62 с.

566. Щедровицкий Г. П. Организационно-деятельностная игра. Сборник текстов (1) / Из архива Г.П. Щедровицкого. — Т9. (1). — М, 2004. — 288 с.

567. Щекин Г. В. Теория социального управления : [моногр.] / Г. В. Щекин. — К. : МАУП, 1996. — 408 с.

568. Эффективность государственного управления: Пер. с английского/ Общ. ред. С.А.Батчикова и С.Ю.Глазьева. — М.: Фонд «За экономическую грамотность», Российский экономический журнал, Издательство А О «Консалтбанкир», 1998. — с.783–810.

569. Эшби У. Р. Введение в кибернетику : пер. с англ. / У. Р. Эшби. — 3-е изд. — М. : КомКнига, 2006. — 432 с.

570. Юзвишин И. И. Информациология или закономерности информационных процессов и технологий в микро- и макромирах Вселенной / И. И. Юзвишин. — 4-е изд., испр. — М., 1996. — 214 с.

571. Юзвишин И. И. Основы информациологии: Учебник / И. И. Юзвишин.— Изд. 2-е, перераб. и доп. — М.: Международное изд-во «Информациология»; «Высшая школа», 2000.— 289 с.

572. Яглом А. М. Вероятность и информация / Яглом А. М., Яглом И. М. — М., 1973.

573. Янковский С. Я. Концепции общей теории информации [Электронный ресурс] / С. Я. Янковский. — Режим доступа:

574. http://n-t.ru/tp/ng/oti.htm. — Загл. с экрана.

575. Aleksander Y. Terrorism, the Media and the Police// Journal of International affairs.Georgetown. 1978. Vol.32. N.1;

576. Bassinouni ,M. Cherif Terrorism, Law Enforcement, and the Mass Media: Perspectives, Problems, and Proposals// Journal of Criminal Law and Criminology. Chicago. 1981. Vol.72, N.1;

577. Bell D. The Coming of Post – Industrial Society: A Venture in Social Forecasting. – New York: Harper/Collins, 1996. – P. 483;

578. Bell D. The Social Framework of the Information Society. Oxford, 1980;

579. Bell D. The Year 2000 — The Trajectory of an Idea / D. Bell // Toward the Year 2000. Work in Progress / Ed. by D. Bell. — Boston, 1968. — P. 5–6.

580. Biernatzki W. E. Terrorism and Mass Media//Center for the Study of Communication and Culture. London. 2002. Vol.21. N.1;

581. Bogason P., Toonen T. Introduktion: Networks in Publik Administration / Publik Administration, 1998, Vol. 76, p. 209–212.

582. Brzezinski Zb. Between Two Ages. N.Y., 1988.

583. Caldwell B. Media Conscience And Accountability // A Free Press: rights and responsibilities / United States Information Agency. June 24, 1997 / http://portal.grsu.by/portal/LIBRARY/CD 1/media /freepr/ essay2.htm

584. Castells M. End of Millennium. Vol.3 of The Information Age: Economy, Society and Culture. Oxford: Blackwell. 1998.

585. Castells M. The Information Age: Economy, Society and Culture. – Maiden (Mac); Oxford (UK): Blackwell Publ. – Vol. 1: The Rise of the Network Society, 1996;

586. Castells M. The Information Age: Economy, Society and Culture: End of Milenium. Maiden (Ma.) Oxford: Blackwell Publ., 1998;

587. Castells M. The Power of Identity. Vol.2 of The Information Age: Economy, Society and Culture. Oxford: Blackwell. 1997;

588. Castells M. The Rise of the Network Society. Vol.l of The Information Age: Economy, Society and Culture. Oxford: Blackwell. 1996;

589. Changing styugins of man. Contract Number URH (489)–2150 Policy Research Report Number 4/4/74, Prepared by SRI Ce nter for the Study of Social Policy, Director Willis Harmon.

590. Cohen F. Terrorism and Cyberspace // Network Security, 2002, Vol.5;

591. Coleman, Dr. John: “Conspirators Hierarchy: The Story of the Committee of 300, America West Publisher, P.O. Box 2208, Carson City, NV 89702.

592. Convey M. Terrorist use of Internet and Fighting Back//Materials of the conference Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. Oxford., 2005;

593. Denning D. E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy// http://www.crimevl.ru. docs/stats/stat_92..htm;

594. Deutsch K. W. Nationalstaat und globale Herausforderung / Karl W. Deutsch. — Stuttgart : Robert-Bosch-Stiftung, 1989. — 30 s. — (Ein Jahrhundert wird besichtigt).

595. Directive № 3-13.1 1995 года. — Режим доступа: (www.fas.org/irp/offdocs);

596. DoD Directive TS-3600.1, "Information Warfare (U)," December 21, 1992 (http://cryptome.sabotage.org/dodd3600-1.htm);

597. Dordick H. S., Wang G. The Information Society: A Retrospective View. Newbury Park – L., 1993.

598. Drucker P. F. The Next Information Revolution // Forbes ASAP. 1998. August 24.

599. Dziundziuk V. Possibilities and Threats Caused by the Development of Information Society // Research papers of Kaunas University of Technology “Public Policy and Administration”. — 2010. — Nr. 33. — P. 9–22.

600. Duverger M. The idea of politics. Indianapolis, 1966. P. 186.

601. Furnell S. , Warren M. Computer Hacking and Cyberterrorism: The real threat in the new millennium.//Computers and Security. 1999. Vol.18 N.1;

602. Galbraith J. K. The New Industrial State. 2 edition. Harmonds worth: Penguin. 1972.

603. Gordon George. Public Administration in America. — 3-d edition. — N. Y. : St. Martins Press, Inc, 1986. — 242 p.

604. Habermas J. Communication and Evolution of Society. Boston, 1979;

605. Hartley R. V. L. Transmission of Information / R. V. L. Hartley // Bell System Technical Journal. — 1928. — No. 7. — P. 535–563.

606. Hartley R. V. L. A New System of Logarithmic Units / R. V. L. Hartley // Proceedings of the IRE. — 1955. — Vol. 43, No. 1.

607. Herbert A. S. The global broadcasting system and the national information policy. Pittsburgh, 1996;

608. http://lidr.undp.org/reports/global/2004/english.

609. http://www.ips-dc.org (Institute for policy studies, IPS);

610. http://www.rand.org (RAND Corporation);

611. http://www.sri.com (Stanford research institute, SRI);

612. Hundley R.O. The Global Course of the Information Revolution: Political, Economic and Social Consequences. RAND, 2000;

613. International Public Information (IPI). — Режим доступа: (www.fas.org/irp/offdocs/pdd/pdd 68.htm)

614. Irvin C. Terrorists Perspectives: Interviews. In Paletz D., Shmid A.. Ed. Terrorism and the media. Newbury Park. 1992;

615. Katz R.L. The Information Society: An International Perspective. N.Y., 1988.

616. Keith S. Fear-mongering or fact: The construction of “cyber-terrorism” in US., UK., and Canadian news media// Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities Oxford, 2005;

617. Lesser J., Hoffman B. Countering the new Terrorism.— Santa Monica, 1999;

618. Lewis J.A. Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats//http://www.crimevl.ru. docs/stats/stat_82.htm;

619. Lockyer A. The relationship between the Media and Terrorism. Canberra, 2003;

620. Machlup F. The production and Distribution of Knowledge in the Unated States. Princeton, 1962;

621. Margulies P. The Clear and Present-Internet: Terrorism, Cyberspace, and the First Amendment.//www.lawtechjournal.com/articles/2004/04_041207_margulies.pdf;

622. Martin L. J. The Media’s Role in international Terrorism// http://pegasus.cc.ucf.edu ~surette/mediasrole.html;

623. Martin W. J. The Global Informational Society. Aldershot: Aslib Gower, Brookfield, Vt, USA, Gower, 1995/ Цит. по: Социум XXI века: рынок, фирма, человек в информационном обществе / Под ред. А.И. Колганова. — М., 1998. — С.32.

624. Masuda Y. The information Society as Post-Industial Society. Wash., 1981;

625. Masmoudi M. The new world information Order. New York, 1983; Masuda Y. The information society as postindustrial society. Washington, DC: World Future Society, 1983.

626. McLuhan M. The Gutenberg Galaxy / M. McLuhan. — New York, 1962.

627. McLuhan M. Understanding media: The Extensions of Man / M. McLuhan. — New York, 1967.

628. McLuhan M. War and peace in the global village; an inventory of some of the current spastic situations that could be eliminated by more feedforward / [by] Marshall McLuhan [and] Quentin Fiore, co-ordinated by Jerome Agel. — New York : McGraw-Hill, 1968. — 190 p.

629. MR-661-OSD. Strategic Information Warfare. A new face of War. (http://www.rand.org/pubs/monograph_reports/MR661);

630. MR-963-OSD. The Day After in the American Strategic Infrastructure. (http://www.rand.org/pubs/monograph_reports/MR 963);

631. MR-964-OSD. Strategic Information Warfare Rising. (http://www.rand.org/pubs/monograph_reports/MR964);

632. Muirie M. Broadcasters Getting Online, Staying On Air // Global Issues: Media Emerging / An Electronic Journal of the U.S. Department of State. March 2006.

633. Naisbitt J. Global Paradox. – New York, 1995; New York, 1996;

634. Porat M., Rubin M. The Information Economy: Development and Measurement. Wash., 1978;

635. Parsons T. Politics and social structure: On the concept of political power. New York, 1969. P. 335.

636. Presidential Decision Directive PDD 68 30 April 1999(www.fas.org/irp/offdocs/pdd/pdd_68.htm) International Public Information (IPI);

637. Riesman D. Leisure and Work in Post-Industrial Society / D. Reisman // Mass Leisure / Eds. E. Larrabee, R. Meyersohn. — Glencoe, 1958. — P. 363−385.

638. Roszak T. The Cult of Information: The Folklore of Computers and the True Art of Thinking. New York: Pantheon Book, 1986.

639. Schmidt-Eenboom, Erich. Nachrichtendienste in Nordamerika, Europa und Japan Länderporträts und Analysen Weilheim. STÖPPEL-Verlag 1995. – S. 3-70.

640. Schmitt K. Der Begriff des Politischen. Berlin, 1963. S. 38.

641. Shannon C. E. A Mathematical Theory of Communication / C. E. Shannon // Bell System Technical Journal. — 1948. — T. 27. — P. 379–423.

642. Shannon C. E. Communication in the presence of noise / C. E. Shannon // Proc. Institute of Radio Engineers. — 1949. — T. 37, № 1. — P. 10–21.

643. Shinder D. Scene of Cybercrime: Computer Forensics Handbook.// http://www.crimevl.ru.docs/stats/stat_97.htm.

644. Smith A.D. National identity. London, 1991.

645. Thomas T.L. Al Qaeda and the Internet: The Danger of "Cyberplanning"//www.iwar.org.uk/cyberterror/resources /cyberplanning/al-qaeda.htm;

646. Wilkinson P. The Media and Terrorism: A Reassessment//Terrorism and Political Violence. London. Vol. 9. N.2.

647. Wilson C. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress//http://www.fas.org/sgp/crs/terror/index..html;