КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
ІНСТИТУТ ЖУРНАЛІСТИКИ

На правах рукопису

ДУБНЯК КАТЕРИНА АНДРІЇВНА

УДК 007 : 304 : 659. 3

СОЦІАЛЬНОКОМУНІКАЦІЙНИЙ ВИМІР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Спеціальність 27.00.01 – «теорія та історія соціальних комунікацій»

Дисертація на здобуття наукового ступеня кандидата наук із соціальних комунікацій

Науковий керівник
кандидат філологічних наук, доцент
Корнєєв Віталій Михайлович

КИЇВ - 2016

ПЛАН

ВСТУП

Актуальність теми дослідження визначається незмінними тенденціями до перетворення інформації в найцінніший глобальний ресурс сьогодення. При цьому, враховуючи інтенсивність впровадження сучасних інформаційних технологій, насамперед, широке використання відкритих інформаційно-телекомунікаційних систем різними суб'єктами (держави, міжнародні організації, фізичні та юридичні особи), суттєво зросла загроза втрати контролю держав над своїм інформаційним полем та суспільною свідомістю громадян. Зазначена проблема постає в першу чергу через відсутність в кордонів в мережі Інтернет, в той час як державам завжди є, що захищати в межах своїх кордонів. Потреба залучення громадськості на свій бік в умовах миттєвого поширення інформації, так само як і дезінформації, використання різними суб'єктами низки методик маніпуляції, методик впливу на формування громадської думки та суспільної свідомості, стала особливо важливою в контексті забезпечення державами інформаційної безпеки. Пріоритетного значення набуває, зокрема, забезпечення чіткості та системності в реалізації державної політики у галузі підтримки і розвитку інформаційного простору, вдосконалення національної інформаційної інфраструктури, організації та забезпечення міжнародного інформаційного обміну й інтеграції інформаційного простору окремих держав (не в останню чергу й України) у світовий інформаційний простір, реалізації принципу рівноправності у взаємодії з іншими державами в інформаційній сфері.

Дослідження природи, сутності та особливостей інформації та інформаційного простору в його соціокомунікаційному вимірі, а також місця і ролі комунікаційних складових системи суспільних відносин, набувають критично важливого значення у зв'язку з виникненням загрози дедалі більшого використання інформаційного простору для задоволення окремих інтересів, створення вигідного для окремих груп людей інформаційного середовища, а також протиправного використання простору. Необхідно

врахувати, що завдяки створенню інформаційних приводів, імперативів та особливостей подачі інформації, сьогодні як ніколи моделюється суспільна свідомість та, в решті-решт, суспільна поведінка.

Актуальність дослідження підсилюється важливістю задекларованого Україною вибору Євроатлантичної інтеграції, а як відомо, Європа сьогодні активно розбудовує інформаційне суспільство. Відповідно, гостро постала проблема ефективного забезпечення інформаційної безпеки молодої держави. Крім того, Україна сьогодні бореться з сусідом-агресором, який веде проти неї гібридну війну, де інформація виступає одним з основних видів арсеналу зброї супротивника. У цьому зв'язку, ефективна та продуктивна координація дій відповідних центральних та регіональних органів виконавчої влади щодо забезпечення національних інтересів нашої держави з протидії реальним та потенційним викликам і загрозам в інформаційній сфері на сьогодні набуває особливого значення.

Різні аспекти теми дисертаційного дослідження були розглянуті в роботах таких вітчизняних та іноземних вчених у сфері інформації, інформаційно-комунікативних технологій, а також їх впливу на суспільство (Ш. Айенгара, Д. Белла, З. Бжезинського, Дж. Донахью, С. Кара-Мурзи, Х. Кепплінгера, Д. Кіндера, Г. Лассвелла, Н. Лумана, Є. Макаренко, М. Маклюена, Д. МакКвейла, Дж. Мілля, Дж. Мільтона, К. Олієна, Ф. Тіченора, Г. Хабермаса, М. Хоркхаймера), дослідників масової і соціальної комунікацій та інформаційного простору (В. Васютіна, В. Гаоптія, В.Городяненко, Л. Городяненко, О. Гриценка, В. Горбуліна, М. Згуровського, Т. Затонацької, В. Іванова, Г. Кривошиї, І. Набруско, І. Надольного, Ю. Перфільєва, В. Різуна, О. Старіша, А. Чічановського, І. Цикунова, Н. Шершньової, В. Шкляра), вчених новітнього напрямку - міжнародне інформаційне право (І. Арістової, А. Пазюка, Г. Віленського), а також інформаційної безпеки (Л. Євдоченка, Б. Кормича, Б. Кузьменка, А. Логінова, О. Носенка, Т. Робінсона, Дж. Франкла, О. Чайковської) та інших.

Нормативну основу дослідження становлять закони та інші нормативно-правові акти, а також національне законодавство України та зарубіжних країн. Особливе місце в дослідженні посідає розгляд доктрин та стратегій інформаційної безпеки низки держав – Канади, США, Японії, Російської Федерації, Естонії, Угорщини, Німеччини, а також України.

Зазначені вище фактори зумовлюють актуальність тему дослідження, а також її важливість як з теоретичної, так і з практичної точки зору.

Зв'язок з науковими темами, планами, програмами. Дисертаційне дослідження виконано в рамках НДР №11БФ045-01 «Український медійний контент у соціальному вимірі» Інституту журналістики Київського національного університету імені Тараса Шевченка.

Мета дослідження. Основною метою дисертаційного дослідження є проведення комплексного і системного аналізу соціокомунікаційного виміру забезпечення інформаційної безпеки держави в контексті стрімкого розвитку інформаційних і комунікаційних технологій.

Задачі дослідження:

- визначити місце і роль інформації в соціальному управлінні;
- здійснити дослідження ролі засобів масової інформації та комунікації в становленні та поведінці соціуму;
- виявити соціокомунікаційний зріз загроз національним інтересам в інформаційній сфері;
- розглянути особливості соціокомунікаційного виміру структурних та функціональних параметрів інформаційного простору, а також дослідити різні комунікативні моделі та, відповідно, запропонувати соціокомунікаційну модель інформаційної безпеки;
- виокремити критерії забезпечення державами національної і громадської безпеки в інформаційному просторі на рівні стратегій (доктрин) інформаційної безпеки з врахуванням соціокомунікаційного виміру на основі порівняльного аналізу стратегій інформаційної безпеки зарубіжних країн;

- охарактеризувати соціокомунікаційну модель інформаційної безпеки у структурі національної безпеки України.

Об'єктом дисертаційного дослідження є соціальнокомунікаційний вимір інформаційно-комунікаційних технологій управління суспільством та інформаційної безпеки держави. **Предметом** дослідження є концепції та стратегії інформаційної безпеки зарубіжних держав, національне законодавство України у галузі захисту інформації та забезпечення національної безпеки в інформаційній сфері, а також наукові концепції та доктринальні доробки на напрямку інформаційно-комунікаційному напрямку та міждисциплінарного характеру.

Методи дослідження становлять систему взаємопов'язаних загальнонаукових та спеціальних інструментів наукового пізнання, застосування яких забезпечує достовірність висновків і розв'язання поставлених завдань.

Історичний метод використовувався при аналізі поняття «інформація», «інформаційне суспільство», «комунікація», а також при дослідженні особливостей становлення інформаційного суспільства та комунікаційних технологій.

За допомогою методу *порівняльного аналізу* вдалось дослідити відмінні риси у врегулюванні та забезпеченні інформаційної безпеки різних державами, зокрема, США, Канадою, Німеччиною, Естонією, Японією та Україною. Крім того, він надав можливість проаналізувати особливості впливу різних способів маніпуляції на становлення та поведінку соціуму.

Діалектичний метод дозволив всебічно дослідити проблеми забезпечення інформаційної безпеки держави як невід'ємної складової національної безпеки держави і дійти висновку, що соціокомунікативна складова в ній набуває дедалі більшого значення і є прямо пропорційною розвитку інформаційних і комунікаційних технологій.

Автор використав *метод індукції* при виокремленні критеріїв ілюстрації забезпечення державами національної і громадської безпеки в інформаційному просторі на рівні стратегій (доктрин) інформаційної безпеки з врахуванням соціокомунікаційного аспекту на основі розгляду окремих стратегій інформаційної безпеки, досвіду держав у ций сфері, а також доктринальних напрацювань.

Метод прогнозування використовувався автором при відстеженні тенденцій розвитку інформаційних і комунікаційних технологій та впливу такого розвитку на інформаційну безпеку держав.

Метод екстраполяції став у нагоді при з'ясуванні, що управління соціальними системами – окремими індивідами та суспільствами в цілому здійснюється завдяки управлінню інформаційним ресурсом з метою задоволення інтересів суб'єкта, який здійснює таке управління, та перенесення відповідних висновків на сферу політики та міждержавних відносин.

Наукова новизна одержаних результатів полягає в тому, що представлена робота є першою у вітчизняній літературі, присвяченій теорії та історії соціальних комунікацій, спробою комплексного дослідження місця соціокомунікаційного аспекту інформаційного простору в забезпеченні інформаційної безпеки держави.

Основні результати, що становлять наукову новизну, відображають особистий внесок автора та виносяться на захист, наступні:

вперше:

- виокремлено критерії забезпечення державами національної і громадської безпеки в інформаційному просторі на рівні стратегій (доктрин) інформаційної безпеки з врахуванням соціокомунікаційного аспекту;

- сформовано соціальнокомунікаційну модель інформаційної безпеки у структурі національної безпеки України;

- на основі порівняння стратегій інформаційної безпеки низки держав, виокремлено критерії соціокомунікаційного спрямування, які мають враховуватись при розробці стратегій інформаційної безпеки держави в цілому;

удосконалено:

- здійснено комплексний аналіз способів та особливостей впливу засобів масової комунікації (далі – ЗМК) та засобів масової інформації (далі – ЗМІ), зокрема, на суспільство, громадську думку та у цьому зв'язку відзначено, що внаслідок тісного взаємозв'язку з політикою, ЗМІ відіграють роль ретранслятора і дзеркала іміджу, що здатен впливати та громадську думку;

- наголошено на тому, що найчастіше до взаємодії зі ЗМІ вдаються як раз в політичних цілях, а також підкреслено, що легітимізація владних дій, створення позитивної громадської думки по відношенню до владних структур, підтримка домінуючих ціннісних орієнтирів у суспільстві залежить від характеру та рівня взаємозв'язків політичних еліт та ЗМІ;

- на основі емпіричних даних, статистичної інформації, аналізу практики та нормативно-правової бази, а також особливому прикладі України, доведено важливість забезпечення інформаційної безпеки на національному рівні з врахуванням реалізації чітко визначеної державної політики відповідно до розроблених та прийнятих стратегій, концепцій і програм у всіх сферах суспільного життя, і в інформаційній сфері зокрема, які б відповідали останнім викликам інформаційно-комунікаційних технологій, з особливим наголосом на вплив соціальних мереж на суспільні процеси;

отримало подальший розвиток:

- дослідження місця й ролі інформації в соціальному управлінні та зв'язку між постійним зростанням обсягів інформації, її впливу на якісний розвиток суспільства і обумовлення поступового переходу суспільства на вищий щабель розвитку, що супроводжується певними викликами для безпеки в більш загальному контексті;

- на підставі аналізу впливу ЗМК на формування громадської думки виявлено, що за допомогою комунікацій і цілеспрямованого систематичного інформаційного впливу на суспільство, в тому числі й з використанням соціальних мереж, можливо реалізовувати різні ідеї, змінювати сприйняття індивідом або суспільством навколишнього середовища, загальноприйнятих людських цінностей, і навіть світу в цілому;

- продемонстровано, що безпека держави полягає у підготовці й превентивних діях з попередження негативних наслідків інформаційно-технологічної революції з відповідним зваженим та всебічним врахуванням таких супутніх особливостей цього процесу як вільний доступ до інформаційних систем; розмивання традиційних кордонів; можливість контролювати сприйняття.

Теоретичне і практичне значення одержаних результатів дослідження полягають у тому, що його наукові положення і висновки сприятимуть подальшому розвитку вчення про соціальні комунікації, інформаційну безпеку, а також можуть бути використані при глибшому вивченні актуальних проблем на напрямку національного забезпечення інформаційної безпеки держави, зокрема, в рамках докторальних досліджень, при написанні монографій та інших наукових робіт.

Матеріали дисертації та сформульовані в ній висновки можуть бути використані в навчальному процесі при підготовці посібників, підручників, методичних матеріалів, курсів лекцій, викладанні нормативного курсу «Соціальні комунікації» та спецкурсу «Соціальнокомунікаційна складова інформаційної безпеки», при підготовці пропозицій владним структурам, зокрема, в світлі розробки та прийняття концепції інформаційної безпеки України, та іншим зацікавленим інстанціям для використання ними у законотворчій діяльності.

З урахуванням того, що в дисертації частково проаналізовані особливості та роль засобів масової інформації в маніпулюванні суспільною думкою,

результати дослідження можуть бути корисними в практичній площині роботи зі ЗМІ, а також для самих представників цієї індустрії.

Особистий внесок здобувача. Дослідження виконане здобувачем особисто, всі результати роботи, сформульовані висновки, положення і рекомендації обґрунтовано на основі особистого доробку автора. Для аргументації окремих положень роботи використовувались праці інших вчених, на які зроблено посилання.

Апробація результатів дисертаційного дослідження. Основні теоретичні та практичні положення й висновки, що містяться в дисертації, обговорювалися на засіданнях кафедри соціальних комунікацій Інституту журналістики Київського національного університету імені Тараса Шевченка. Положення дисертаційного дослідження автор використовував в навчальному процесі, зокрема, при викладанні практичних занять в Інституті журналістики Київського національного університету імені Тараса Шевченка.

Теоретичні та практичні результати дисертаційного дослідження доповідалися та обговорювалися на 4 міжнародних та всеукраїнських наукових конференціях: Всеукраїнська науково-практична конференція «Сучасні виклики для соціально значущої медіа діяльності», місто Київ, Інститут журналістики КНУ імені Тараса Шевченка, 26-27 березня 2015 року; Міжнародна науково-практична конференція «Стандарти журналістики та професійної освіти в період суспільних трансформацій», місто Львів, ЛНУ імені Івана Франка, 23-24 квітня; Міжнародна наукова конференція «Інформація, комунікація, суспільство 2015», місто Львів, Національний університет «Львівська політехніка», 20-23 травня; Міжнародна наукова конференція «Actual problems of science and education», організовану «Society for Cultural and Scientific Progress in Central and Eastern Europe», місто Будапешт, Угорщина, 2016 рік.

Публікації. Основні положення та висновки дисертаційного дослідження відображені у 5 одноосібних статтях, опублікованих у фахових наукових виданнях, зокрема, одній опублікованій за кордоном, та в тезах доповіді на науковій конференції.

Структура дисертації зумовлена предметом, метою, завданнями та логікою дослідження обраної теми. Обрано структуру дисертації, яка містить вступ, три розділи, що об'єднують дев'ять підрозділів, висновки та список використаних джерел. Загальний обсяг дисертації становить 205 сторінки, список використаних джерел викладений на 22 сторінках, який нараховує 200 найменувань.

РОЗДІЛ 1
СОЦІАЛЬНО-КОМУНІКАЦІЙНІ ФУНКЦІЇ ІНФОРМАЦІЇ В УПРАВЛІННІ СУСПІЛЬСТВОМ

1.1. Місце і роль інформації в соціальному управлінні

Розвиток інформаційних технологій став черговою сходинкою в еволюції людства. Інформаційні технології та технічні засоби, побудовані на їх основі, проникли у всі інститути суспільства та сфери життєдіяльності людини. Вони розвивались паралельно зі зростанням світової економіки. Як зазначає О. Зернецька, природа нових глобальних трансформацій широко визначається тим фактом, що людство входить до нової ери розвитку – ери складних процесів революції комунікації та інформаційного буму, які призводять до установлення нового світового порядку [1].

Інформаційні та комунікаційні технології розглядаються різними міжнародними інституціями як [2]:

- сполучна ланка між розвинутими країнами та країнами, що розвиваються [3];
- інструмент для економічного і соціального розвитку [4];
- енергія для стимулювання зростання [5];
- основний стовп для формування глобальних економічних і соціальних знань [6];
- можливість для країн позбутися наслідків несприятливого географічного положення [7].

Сучасний стан розвитку інтелектуальної еліти цивілізації можна з упевненістю охарактеризувати як інфосферу, через те, що внаслідок, прискореного, всеосяжного розвитку і розповсюдження глобальних телекомунікаційних систем формується середовище існування людства [8, 25].

Інформація та технології змінили розуміння часу простору та в цілому буття, інформаційна складова діяльності людей переважає над всіма іншими її формами і компонентами. Від якості інформації став залежним розвиток технологічного устрою держави та суспільства. Поступово удосконалюються технології передачі інформації і засоби комунікації, спрямовані на широкий загал. Високі технології, економіка, наука, культура й інформація стають взаємодоповнюваними.

Обсяги і вплив інформації на продуктивний розвиток суспільства дедалі зростають. Як зазначає професор А. Чічановський «інформаційні технології стають основною рушійною силою нової соціально-технологічної системи і містять серйозні наслідки для еволюційних соціальних процесів. І хоча сама по собі інформатизація не вирішує головних проблем становлення соціуму, відносини людини з інформаційним середовищем зумовлюють радикальні трансформації в людині, і як наслідок, - у цивілізації в цілому» [8, с. 50].

Локальна інформатизація суспільства інтегрується у глобальну систему. Суспільство отримує доступ до глобальних джерел інформації і систем її обробки. Поєднання нових інформаційних технологій і широкий доступ до їх використання переводить людство до нового ступеня розвитку інформаційного суспільства.

Поступово суспільство насправді переходить на вищий щабель розвитку. Так, на початок XXI ст. припадає розвиток особливого, відмінного від раніше існуючих, суспільства - суспільства інформаційного, - яке пропонує активний розвиток та доступність широкому загалу (також для незаможних верств населення) інформаційні і комунікаційні технології. Створюються умови для ефективного використання знань та інформаційних технологій у вирішенні найважливіших завдань управління суспільством і державної систематизації суспільного життя. Світова спільнота на чолі з суверенними державами, ставши на шлях постіндустріальної цивілізації становлення і розвитку інформаційного суспільства, формує різні шляхи його побудови.

Дійсно, на перший погляд завдання дати вичерпне та всеохоплююче поняття терміну «інформаційне суспільство» може видатися доволі легким. Однак, при цьому слід мати на увазі та усвідомлювати безліч нюансів, концепцій та підходів, які висувають не тільки науковці в межах однієї галузі науки, а й різні науки. Тим не менше, аналіз такого складного феномену видається вдалим розпочати із з'ясування поняття «інформація».

Розглянемо поняття «інформація». Перш за все, слід зазначити, що навряд чи можна відшукати універсальне визначення цього поняття, адже вчені по-різному його тлумачать. Однак, насправді дискусії точаться тільки довкола *змісту* поняття «інформація», непорозумінь стосовно використання саме відповідника «інформація» в науці не спостерігається.

Так, Н. Вінер вважав, що «інформація — це позначення змісту, який надходить з зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів» [9, с. 31].

Пануючі у закордонних учених точки зору на інформацію добре систематизував Ф. Махлуп:

«1) інформація — процес передачі знань, сигналу чи повідомлення;

2) інформацією є поточні дані про перемінні величини в деякій галузі діяльності, систематизовані відомості щодо основних причинних зв'язків, котрі містяться у знанні як понятті більш загального класу, по відношенню до якого інформація є підлеглою;

3) інформація є знання, які передані кимось іншим чи набуті шляхом власного дослідження чи вивчення;

4) інформація є знання про якусь особу подію, випадок чи щось подібне» [10].

Крім того, в науці поширені різні погляди на природу інформації. В цьому ключі, одним з підходів є ідея щодо двох якісно різних видів інформації — докібернетичного і кібернетичного. Основою цієї теорії служить твердження про різницю інформативної природи живої та неживої

матерії. Так, Д. Дубровський цікаво трактує відмінність між сигналом та інформацією; він зазначає, що ця різниця лежить в основі виділення двох процесів — того, що відбувається на допсихічному рівні та на рівні людської психіки. На рівні кібернетичної системи, яка ще не досягла висот психічного розвитку, сигнал та інформація злиті воєдино і використовуються разом, а що стосується системи, яка має здатність до психічного управління, «то на рівні психічного управління відбувається ніби роздвоєння єдиного, виділення інформації з сигналу, яке здійснюється у суб'єктивній формі (що рівнозначно виникненню суб'єктивної форми відбиття» [11].

Загалом, коли йдеться про інформацію в докібернетичних системах, деякі автори висловлюють думку про те, що краще було змінити у цьому випадку термін «інформація». Так, Р. Акоф і Ф. Емері зауважують, що К. Шеннон, який запозичив термін «інформація» з праць Хартлі 1928 року, вживав його «переважно в обмеженому (технічному) значенні» [12]. К. Черрі висловився ще більш категорично: «…в деякому розумінні шкода, що математичні поняття, які йдуть від Хартлі, взагалі були названі «інформацією» [13]. Щодо того, як називати це явище у кібернетичних, тобто і в соціальних системах, то тут суперечок немає.

Не викликає сумніву, що інформація, якою обмінюються члени суспільства, обов'язково пов'язана з певним відбиттям реальності. Так, Н. Вінер під інформацією розумів позначення змісту, який надходить із зовнішнього світу у процесі пристосування до нього людини [14]. При цьому, слід вказати на різницю у ставленні до пошуку та обробки інформації людини та машини [14].

Цікавим видається поділ інформації на семантичну та естетичну: семантична – це «інформація, яка підлягає універсальній логіці, має структуру, допускає точне уявлення, яку можна перекласти на інші мови»; естетична — це «інформація, яку не можна перекласти, яка належить не до універсального набору символів, а тільки до набору знань, спільних для

сприймача та передавача; вона теоретично не перекладається на іншу «мову» чи у систему логічних символів тому, що іншої такої мови для передачі цієї інформації просто не існує» [15].

В свою чергу, соціологи розглядають інформацію «як соціальне явище, тобто певний феномен, пов'язаний з діяльністю тих чи інших суб'єктів соціальних спільнот (наприклад, груп) чи соціальних інститутів (наприклад, установ і організацій, які функціонують у суспільстві)» [16]. У соціології поняття інформації не набуває якогось якісно нового змісту, хоча і неповністю використовується в тому ж значенні, як у теорії інформації, бо в обов'язковому порядку передбачає розгляд змісту інформації, що аналізується. В цілому під інформацією в соціології розуміється «будь-яке повідомлення (текст), яке вміщує якісь відомості (нове знання) відносно того чи іншого об'єкта (предмета повідомлення)» [16].

В цілому, особливість інформаційного обміну в соціальних системах полягає в першу чергу в тому, що такий обмін здійснюється саме між індивідами або їх групами. При цьому, технологічним здобуткам та технічним системам відведена роль комунікатора – тобто каталізатора для ефективного та зручного обміну інформацією.

Виходячи з соціологічного підходу до тлумачення інформації можна виділити певні властивості інформації, характерні саме для соціальних систем:

- здатність впливати на психіку (як самостійний об'єкт шляхом участі у психічних процесах бере участь у формуванні нового знання або уявлення);
- значущість (інформація зберігає свою цінність протягом певного терміну):
- достовірність (відповідність інформації дійсності);
- цілісність (її незмінність в умовах випадкових або свідомих дій у процесі інформаційного обміну) [8, с. 116].

Більше того, інформація будується шляхом поступового ускладнення більш простих процесів та набуття ними нових якостей, таким чином ускладнюючись та розвиваючись. Так, складні організми (багатоклітинні) і в першу чергу люди набувають здатність інформаційно взаємодіяти з оточуючим середовищем, одержуючи та передаючи інформацію цілеспрямовано, що в свій час призвело до виникнення соціальних утворень як самостійних об'єктів відносно навколишнього середовища.

Треба зауважити, що глобальною проблемою сучасності стала інформація, адже від неї безпосередньо залежить успішний розвиток суспільства. Крім того, «інформаційна взаємодія різних груп суспільств — найважливіша форма соціальної взаємодії». Адже, як влучно зазначає В. Чічановський, «еволюція соціумів пов'язана саме з розвитком засобів і технологій інформаційної взаємодії його членів, особливо з побудови і використання їх спільної пам'яті», що підводить нас до важливого усвідомлення того, що соціум розвивається з більш відчутним прогресом у порівнянні з його окремими представниками-індивідами [8, с. 103].

Масова інформація — це така інформація (відомості, дані, знання), яку оприлюднено і при цьому вона може бути як документованою, тобто записаною на носії інформації, так і недокументованою (наприклад, виголошена промова) [17]. В будь-якому випадку, це систематизована інформація, яка оперативно та регулярно поширюється на велику, географічно розпорошену аудиторію. Варто зазначити, що серед джерел масової інформації фігурують кіно, театри, концертні зали тощо. Проте, мас-медіа або засіб передачі масової інформації, детальніше про які йтиметься далі, є основним джерелом масової інформації. Все ж слід мати на увазі, що масова інформація є значно ширшим поняттям, ніж та інформація, яку розповсюджують ЗМІ.

Природа масової інформації безпосередньо залежить від характеру діяльності людей у різних соціальних сферах. При цьому соціальна

інформація поділяється на підвиди, покликані відобразити її специфіку - економічна, політична, науково-технічна, художня, релігійна та ін.

Соціальний характер циркулюючої в суспільстві масової інформації обумовлений факторами, що визначають її сутність і специфіку:

- зміст (як певна інформація відображає суспільні процеси);
- суб'єкт використання (як дана масова інформація використовується людьми в їх інтересах);
- специфіка звернення (як така інформація отримується, фіксується, обробляється і передається).

Цікаво також виділити і таке поняття як інформаційні матеріали. Це сукупність джерел та систем, що містять інформацію, призначену для передачі. За формою подання вони поділяються на:

• текстові інформаційні матеріали: документи, книги, журнали, газети, довідники, каталоги, рукописи;

• графічні або образотворчі: графіки, креслення, плани, схеми, карти;

• аудіовізуальні: звуко- та відеозапис, кінофільм, діапозитив, фотографія;

Поширення інформаційних матеріалів ведеться спеціальними підрозділами спецслужб та (або) за їхніми матеріалами – засобами масової інформації.

Так, інформація, в тому числі і масова, є певним продуктом, за який людина може платити або все ж отримувати безкоштовно, в залежності від специфічних факторів. Наприклад, за один вид інформації люди мусять платити (книги, журнали, музика), а за другий платити не доводиться (скажімо, за різні види реклами). Як правило, платять за ту інформацію, яка задовольняє особливі потреби людини: емоційні, естетичні, пізнавальні чи навчальні. За інформацію, яка закликає чи примушує людину до чогось (пропагандистська й рекламна інформація різних видів), як правило, поширюється безоплатно, а розповсюджуючи таку інформацію, її виробники

самі повинні турбуватися про те, щоб реципієнти всупереч їх спротиву цю інформацію сприймали [17].

Таким чином, інформація є продуктом, який має собівартість і ціну, адже його виробляють так само як і будь-який інший матеріальний продукт. Однак, особливість такого продукту полягає в тому, що він виготовляється один раз, а далі може лише копіюватися, а також він не з часом не зникає, як інші матеріальні речі, хіба що може втрачати актуальність.

Інформаційний чинник в останні роки спричинив революційні зміни. Зараз увесь світ включений в єдину інформаційну систему, причому вона працює фактично в режимі реального часу. Інформація для людства є не тільки умовою, але й стимулом до дії, дезінформація та інформаційний хаос викликають почуття невпевненості і безсилля. Велику роль у самопочутті суспільства відіграє також міра задоволення потреби в інформації. У нездоровому суспільстві, як правило, є почуття інформаційного голоду [14].

У соціальному середовищі постійно створюються, затверджуються і трансформуються високі технології, які проектуються на структури соціальних цінностей. Фактично такі технології формують стратегію розвитку цивілізації з її культурною та духовною сферами. Створення інформаційного суспільства у поєднанні з інформатизацією є новим етапом розвитку людської цивілізації, і він не мислимий без розвитку процесу інформатизації, який, у свою чергу, пов’язаний з розвитком інформаційної індустрії, виробництвом як технічних засобів так і програмного забезпечення.

Автор пропонує перейти до безпосереднього розгляду терміну «інформаційне суспільство», в основі якого лежить вище проаналізоване поняття «інформація».

Парламентська Асамблея Ради Європи у 1997 р. визначила термін «інформаційне суспільство» як суспільство, яке ґрунтується на інформації. Термін «інформаційне суспільство» увійшов у вжиток у ході розвитку

інформаційно-комунікаційних технологій (Інтернет, мобільний зв'язок, електронне листування) і, як правило, застосовується для позначення тих аспектів сьогодення, які зазнають найбільшого впливу від таких технологій. Наприклад, швидкість та поширення сучасних ринкових відносин залежить від нових технологій або ж вплив швидкості та якості обробки інформації на рівень зайнятості та благополуччя населення [18, с. 8].

Концепція інформаційного суспільства розроблялась, насамперед, для вирішення завдань економічного розвитку, що зумовило її дещо обмежений і прикладний характер. Однак ця концепція охоплює й ідеологічні та виховні цілі, тому що її реалізація припускає можливість управління індивідуальною й масовою свідомістю за допомогою інформаційних технологій. Це зумовило необхідність формування чіткої позиції суспільства щодо культури, духовності, моралі.

«Інформаційне суспільство - ступінь в розвитку сучасної цивілізації, що характеризується збільшенням ролі інформації і знань в житті суспільства, зростанням частки комунікацій, інформаційних продуктів і послуг у валовому внутрішньому продукті, створенням глобального інформаційного простору, що забезпечує ефективну інформаційну взаємодію людей, їх доступ до світових інформаційних ресурсів і задоволення їх соціальних і особових потреб в інформаційних продуктах і послугах».

Так, як природно слідує з вищезазначеного, термін «інформаційне суспільство» було створено для позначення спільнот, які мають безпосередній доступ до інформації і знань, завдяки чому забезпечуються сталі та рівні можливості для розвитку і прогресу. Для інформаційного суспільства характерний вільний двосторонній обмін інформацією (комунікація) між урядом та народом та, власне, в самому соціумі. В такому соціумі кожен поінформований про перебіг останніх подій, особливо таких, що торкаються представників суспільства безпосередньо. Крім того, кожен має можливість висловитися та бути почутим. Відповідно, кожен індивідуум

впливає на формування та коректування соціально-економічних планів та стратегій національного значення [18].

Рисами інформаційного суспільства є: пріоритетне значення інформації порівняно з іншими ресурсами; домінування інформаційного сектору в загальному обсязі валового внутрішнього продукту; формування й використання нових телекомунікаційних та комп'ютерних технологій. У зв'язку з цим інформаційне суспільство може бути визначено як суспільство, в якому основними предметами праці більшості людей є інформація і знання, а знаряддями праці та управління соціальними процесами є інформаційні технології. Однак за сучасними інформаційними технологіями стоїть більш складна реальність – соціальні інститути, людська діяльність, цінності та відповідні їм картини світу.

Інформаційне суспільство володіє всіма основними характеристиками постіндустріального суспільства (економіка послуг, центральна роль теоретичного знання, орієнтування на майбутнє, розвиток нової інтелектуальної технології). Вирішального значення для економічної та соціальної сфери, для способів здобування знань, а також для характеру трудової діяльності набуває становлення нового соціального устрою, заснованого на телекомунікації.

Розвиток інформаційних технологій, технічних та програмних, тісно взаємопов'язаний із процесом інформатизації суспільства. Основними цілями інформаційного суспільства є блага та переваги, які може привнести інформація, а саме економічний розвиток, індивідуальні можливості, краще медичне забезпечення, участь в управлінні державою [18, с. 8]. Відповідно, громадський сектор не міг залишатися осторонь впровадження та розповсюдження переваг від розвитку інформаційного суспільства та прагнув максимізувати їх, особливо в необхідному та корисному для суспільства ключі.

Так, громадські організації лобіювали проведення Світового саміту інформаційного суспільства або ССІП (англ. - World Summit on the Information Society або WSIS) з метою визначити засоби масової інформації (далі – ЗМІ) частиною інформаційного суспільства. Наприклад, в серпні 2003 р. Африканська медійна конференція «Хайвей Африка» обрала основною темою поширення медіа серед інформаційного суспільства, а заключна декларація конференції пропонувала розширити концепцію інформаційного суспільства і включити такі пов'язані з засобами масової інформації питання як свобода слова, доступ до інформації та ролі журналістики, тобто не обмежуватись лише роллю інформаційних і комунікаційних технологій [19]. Таким чином, про особливо важливу роль ЗМІ було заявлено промовисто та однозначно, цим самим підкреслено його важливо роль для суспільства.

Як визначає резолюція Генеральної Асамблеї ООН 56/183 серед цілей ССІП є вироблення «спільного бачення та розуміння інформаційного суспільства» та прийняття на основі такого спільного бачення та розуміння декларації, яка б містила основоположні принципи для створення справжнього глобального інформаційного суспільства [19].

Відомо, що при виборі напрямку розвитку обов'язково враховуються ті поняття блага та ідеали, на які орієнтовані різні форми діяльності суспільства. Якщо досліджувати розвиток технічних параметрів та засобів передачі інформації, в тому числі в мережі Інтернет, не враховуючи ціннісних критеріїв поданої інформації, то до цього розвитку можна застосувати поняття прогресу. Якщо ж цю інформацію розглядати з погляду моральної рефлексії, то виявиться, що в її загальному потоці домінує негативна і навіть відверто аморальна інформація. У такій ситуації єдиний інформаційний простір, надмірність інформації, відкритий доступ до неї спрацьовують не на усунення кризи духовності, моралі й моральності, а скоріше навпаки – сприяють її різкому посиленню. Саме тому в інформаційному суспільстві особливо гостро стоїть проблема розвитку та

самоідентифікації особистості, яку в нинішній ситуації надлишку інформації (високий рівень розвитку ЗМІ) та комунікації, інформаційних технологій, що цілеспрямовано впливають на самосвідомість людини та культури, реалізувати іншими способами дуже важко.

Тобто, як бачимо, в сучасному суспільстві, де головним ресурсом виступають інформаційні технології, ЗМІ виконують роль формуючого чинника в процесі самоідентифікації особистості, ототожнюючи поняття культура та інформація. Справляючи вплив на кожну окрему людину, засоби масової інформації таким чином долучаються до формування громадської думки і тим самим визначають шляхи розвитку всього суспільства.

«Найголовнішим ресурсом розвитку суспільства є люди, їхні інтелектуальні, творчі, духовні здібності. Сьогодні найбільш обмежений і найдорожчий ресурс - знання й компетенції. Завдання суспільства - створити умови для реалізації потенціалу кожної людини за допомогою інформації, знань, інформаційно-комунікативних технологій» [20].

Використання «оптимальної суміші технологій» вважається ключовим елементом для установлення інформаційного суспільства [21]. Необхідно використовувати різні технології та устаткування, які враховують місцеві умови та такі зміни як злиття технологій [22]

Процес формування інформаційного суспільства охопив наступні сфери: державні установи та підприємства, освітні заклади, інститути громадянського суспільства, комерційні суб'єкти. Як вказується у Валлеттській та Стамбульській деклараціях, злиття технологій є шляхом до нових перспектив в інформаційно-комунікативному секторі: електронне навчання, електронна комерція, електронний уряд, електронна медицина, захист навколишнього середовища, повоєнна відбудова з використанням технологій та багато інших можливостей, які є надзвичайно вигідними для соціального, культурного і економічного розвитку [23]. Як приклад, можна розглянути ціль створення електронного уряду. Так, недостатньо розвинута

мережа та інфраструктура ускладнюють процеси взаємодії між урядом та громадянами в багатьох куточках світу. Електронний уряд покликаний вирішити цю проблему. Використання інформаційно-комунікаційних технологій в урядуванні сприяє розвитку демократії, прозорості та відкритості, а також може підвищити можливості в залученні нових інвестицій та фінансових вливань для країн. Як було відмічено на конференції з електронного урядування в Палермо, інформаційно-комунікаційні технології мають потенціал надзвичайно широко забезпечити участь в політичних процесах, а також підвищити доступ до інформації про діяльність уряду та полегшити доступ до знань [24.].

Основний етап формування інформаційного суспільства це процес стандартизації та систематизації впровадження інформаційних технологій як з'єднувальної ланки - елементу спілкування між державою та суспільством та національно-інформаційних суспільств в інформаційній цивілізації. Так, стандартизація однією з важливих складових глобального поширення телекомунікацій: стрімке впровадження процесів стандартизації що проводилася міжнародними організаціями має сприяти розвитку сучасних та та ранкових стандартів. У той час як процес стандартизації є міжнародним по природі, все ж не можна не відзначити роль приватного сектору. Так, у ході саміту G7 підтверджено, що співпраця між усіма суб'єктами має ґрунтуватися на діалозі під егідою приватного сектора, завдяки якому легше виокремляться слабкі місця.

Людство перейшло в епоху розвитку інформаційного суспільства і отримало таким чином могутній інструмент для об'єднання зусиль з метою одержання нових знань, спрямованих на рішення своїх глобальних проблем, економічного зростання і підвищення життєвого рівня населення.

1.2. Динаміка комунікаційних складових системи суспільних відносин.

Сьогодні наявною тенденцією є швидке зростання ролі інформації в житті суспільства. Це зумовлено бурхливим розвитком високих технологій усіх галузей виробництва та накопиченням досвіду ринкових відносин. Деякі вчені вважають, що інформація за своїм обсягом і важливістю є продуктом, який можна порівняти з усіма іншими продуктами нашої цивілізації. Від неї залежить успішний розвиток суспільства. Володіння інформацією стало визначальною передумовою успіху за умов жорсткої ринкової конкуренції; технологічні вдосконалення, винаходи, ноу-хау перетворились у цінний товар. Інформаційні ресурси, інформаційна інфраструктура і інформаційні технології значно впливають на рівень і швидкість соціально-економічного, науково-технічного і культурного розвитку.

Інформаційна взаємодія різних груп соціуму - найважливіша форма взаємодії. Від її наявності залежать і способи розв'язання тієї чи іншої проблеми. Інформація розглядається як первинний продукт, який треба переробити для отримання інших продуктів без якого неможливо отримання інших продуктів.

Інформація і комунікація є двома рівнями процесу спілкування. Перший – пізнавальний, пов'язаний з поширенням соціально важливих відомостей серед широкої аудиторії. На другому рівні процесу спілкування одержана інформація поєднується з системою існуючих норм і цінностей у суспільстві. Виходить, що процес комунікації має безпосереднє відношення до соціальної дії. Так, комунікація є однією з базових умов існування людської спільноти і поширення інформації. Комунікація походить від латинського слова *communicatio* (зв'язок, повідомлення) і означає передавання інформації від носія (людини), групи носіїв (системи) іншому/іншим за допомогою сигналів чи спеціальних технічних засобів або *communicare*, що означає «бути у зв'язку, брати участь, поєднувати». Англійські відповідники цього терміну, від якого власне він і з'явився і в українському вжитку, це - *communicate*,

community, communication та інші спільнокорінні слова або синоніми – *intercourse*. Серед українських синонімів варто виділити такі слова як: сполучатися, спілкуватися, спілка, спільнота, спілкування. В свою чергу, російські відповідники – це «общий, общество, общаться, общение, приобщить».

Під актом особової, опосередкованої або масової комунікації розуміється певний процес. В історичній ретроспективі комунікація в найпростішій формі розумілась як процес передачі інформації від одного суб'єкта іншому по певному каналу, який зазвичай здійснює вплив певного роду [25, с. 23]. «Комунікація здійснюється одним або ж усіма наступними способами: дія, спрямована на інших, взаємодія з іншими людьми і реакція на дії інших людей». Комунікація - це обмін інформацією між двома або більше людьми, процес передачі інформації від відправника до одержувача через певний канал, який зазвичай певною мірою впливає на споживача. Спілкуватися означає бути членом суспільства, а отже бути з усіма на «одній хвилі» та слідувати визначеним таким суспільством правилам поведінки з метою нормального співіснування. Основним фактором є духовний зв'язок між членами спільноти, однак мова не йде про фізичний зв'язок – наявність духовної єдності та існування різних форм єднання утворюють спільноту [26, с. 7].

Навряд чи можна зосередитись і зупиниться лише на одному підході до розуміння терміну «комунікація». Комунікація притаманна не тільки соціальним системам, але й світу тварин, а також системам механізмів, утворених внаслідок людської діяльності. Термін «комунікація» в технічному середовищі використовується в множині – комунікації (кабельна система телефонної мережі; оптоволоконна система; транспортні комунікації тощо). Дійсно, розглядаючи комунікацію під таким кутом зору домінантним акцентом є зв'язок як індикація згаданого терміну.

В той же час, суспільна комунікація є абстрактним поняттям. В тваринному світі комунікація є дещо примітивнішою, ніж в людському світі та визначається як біологічна поведінка, як реакція пристосування до навколишнього середовища. Прикладом комунікації в тваринному світі є жести, найпростіші звуки, рухи, запах, нюх. Виходячи з цього, можна стверджувати, що засоби комунікації поведінки виникають здебільшого з інстинктивної поведінки. Як у світі людини так і у тваринному світі комунікативний процес є основою спілкування. В суспільстві комунікативний акт є головним для його існування без комунікативної взаємодії не може існувати суспільство.

Справедливо стверджувати, що дедалі важливішого значення набуває комунікація як механізм, що забезпечує існування та розвиток людських відносин (різноманітні символи, що продукуються розумом і передаються крізь простір і час). Цей механізм включає вирази обличчя, жести, тональність голосу, слова, писемність, друк, залізна дорога, телеграф, телефон, дещо ще що може заполонити простір та час [26, с. 11].

Дія будь-якого виду комунікації залежить від умов, в яких відбувається процес комунікації: сприйняття слухачів, читачів та глядачів і від багатьох інших факторів. Деякі з них можуть чинити перепони нормальному засвоєнню інформації, таким чином послаблюючи вплив комунікації чи зовсім нейтралізуючи її. Наприклад, якщо одна людина розповідає іншій анекдот, а інший в цей час відволікає її увагу, вона може пропустити ключову фразу і суть жарту залишиться незрозумілою для неї. Так само, можна думати про щось стороннє під час кіносеансу і не звертати уваги на те, що відбувається на екрані, залишаючи сюжет без уваги.

Комунікація сприяє розвитку людини і є прямо-пропорційною рівню її соціалізації, адже комунікація розвивалась і вдосконалювалась так само як розвивалась і вдосконалювалась людина. В основі такого розвитку лежить комунікативний процес, який є невід'ємною частиною комунікації. Серед

інших елементів, які характеризують комунікацію як системне явище необхідно зазначити наступні:

- Комунікант (суб'єкт комунікації - відправник, особа, збирає інформацію і передає її та одержувач, або особа, якій призначена інформація і який інтерпретує її);

- Комунікат (предмет комунікації - повідомлення, сама інформація, представлена в тій чи іншій формі);

- Комунікативні засоби (канал, або засоби передачі інформації - знакові системи, засоби комунікації)

В свою чергу, як комунікант – відправник інформації та комунікант – одержувач інформації в науковій літературі та на практиці ідентифікуються також як комунікатори.

Комунікаційний процес - це обмін інформацією між окремими людьми або групою осіб. Основна мета комунікаційного процесу - це забезпечення розуміння посланого повідомлення. У процесі обміну інформацією є чотири основні обов'язкові елементи:

Однак, процес комунікації складається з більшого числа елементів і етапів. У відправника спочатку повинна зародитися ідея, чи це можна сформулювати як «спочатку думай, а потім кажи». Повинно бути продумано, яку думку збираються донести до одержувача, чому і яким чином це повинно бути сприйнято. Наприклад, якщо передається інформація про подання нового товару споживачеві, то визначається, що йому треба знати про товар, чому йому потрібен цей товар і яким чином цей товар принесе найбільшу користь.

Таким чином, обробляючи ідею «від одержувача», народжується інформація, яку необхідно представити в будь-якому вигляді або, інакше кажучи, зробити кодування. Кодування - це переклад інформації в слова, символи, інтонацію, жести (мова тіла). Кодування залежить від того, який канал або засіб передачі буде вибрано: вербально, письмове звернення, знак,

плакат, канал електронної комунікації (комп'ютерний зв'язок). Якщо канал не відповідає ідеї, що з'явилася на початковому етапі, обмін інформацією буде неефективний. Наприклад, якщо потрібно пояснити, як працює нове обладнання, можна зробити це вербально, або написавши певну інструкцію. Якщо процес роботи складний, то другий канал комунікації буде більш ефективним, особливо якщо він підкріплений візуальною інформацією (малюнками і графіками).

Вибір засобу повідомлення не повинен обмежуватися єдиним каналом. Бажано використовувати два або більше засобів комунікації в поєднанні. Це може підсилити ефект сприйняття і виправити недоліки якогось одного каналу. Важливим фактором, що впливає на комунікаційний процес, є організаційний аспект, а саме конфігурація комунікаційних мереж. Мережі - це з'єднання, що відповідним чином беруть участь у комунікаційних процесах індивідів або елементів за допомогою інформаційних потоків і характеризуються тим, що один з членів групи завжди знаходиться на перетині всіх напрямків спілкування.

Розуміння цих типів комунікаційних мереж важливо при визначенні владних повноважень і соціальних позицій в групі.

Передача інформації одержувачу - це фізичне доведення інформації до одержувача, яке часто приймають за весь процес комунікації. Фактично, це процес організації доступності інформації або інформаційного повідомлення і, як правило, цей процес здійснюється особами (секретарями, посильними, поштарями) або електронними засобами (електронна пошта, повідомлення в соціальній мережі). Однак, найголовніший аспект: одержувач (наприклад, виконавець або начальник) повинен побачити, почути і зрозуміти те, що йому повідомляють.

Розуміння залежить від того, як відбувається декодування інформаційного повідомлення. Декодування - це переклад символів відправника в думці одержувача. Чим точніше символи обрані, тим точніше

вони будуть декодовані. Кожен керівник повинен підбирати такі вираження своїх думок, які відповідають рівню сприйняття підлеглого.

Весь процес передачі інформації був би неповним без отримання (контролю) та інтерпретації зворотного зв'язку. Після отримання повідомлення в одержувача виникає реакція, яка характеризує те, як було зрозуміле повідомлення. Одержувач виробляє дію, яка також має бути декодована, але вже самим відправником. Виникає зворотний зв'язок, що дозволяє контролювати і коректувати процес передачі інформації. Зворотній зв'язок підвищує ефективність всього комунікаційного процесу.

Виділяють три основні етапи розвитку комунікації: доіндустріальний; друкарський та телевізійний, на якому автор зупиниться детальніше в наступному підрозділі.

Крім того, варто виокремити форми комунікації, які визначаються структурою та характером комунікативного процесу. Виділяють одно- і багатовекторні процеси спілкування. Так, одновекторна комунікація відрізняється постійністю ролей комуніканта і комуніката і є характерною для неформального спілкування, однак використовується і в наукових та виробничих колах. В свою чергу, багатовекторна комунікація характеризується постійною зміною вищезгаданої ролі комуніканта (він може бути і відправником і одержувачем інформації), а також має діалогічну форму спілкування [8, с. 140].

В межах згаданих векторів фігурують такі типи спілкування як:

- Монолог; Діалог; Групова комунікація; Групова комунікація; Ринково-медійна комунікація Віртуальна комунікація [8, с. 141-142].

Засоби комунікації є не тільки трансляторами або ретрансляторами даних, це також субстанція з відповідно заданими координатами, що впливає на свідомість людини та соціуму. При цьому, все ж видається важливим окремо зупинитися на одному з найбільш відомих засобів комунікації, який

фактично є найбільш розповсюдженим і найбільш широко вживаним серед практично усіх соціумів – мові. Мова - це система знаків, що визначає правила побудови особливих різноманітних інформаційних кодів, які підтримують життєздатність інформаційної системи та забезпечують її функціонування в цілому [8, с. 103]. Такими інформаційними знаками-кодами позначаються різні явища, об'єкти, суб'єкти тощо. В процесі мовлення (тобто спілкування або використання мови в комунікації) відбувається обмін певної інформацією, що міститься в згаданих інформаційних кодах, можна навіть сказати, що відбувається процес її декодування. Цікаво, що мається на увазі не лише мова вербальна, а також і невербальна – мова жестів, мова культури, мова програмування тощо. Для кожного з цих підвидів існує свій набір кодів або знакова система, що роблять її особливою та унікальною.

Вербальна мова є усною та письмовою, а невербальна може бути первинною та вторинною. Первинні мови – це мови жестів, міміка або пантоміма; вторинні мови – всім добре відома азбука Морзе, музична нотація, згадана мова програмування [8, с. 153]. Невербальна мова часто використовується невимушено, а якщо особи можуть «читати обличчя», то часто завдяки розпізнаванню та декодуванню жестів та міміки вони можуть «читати» інших людей.

Цікаво зазначити, що не дивлячись на її виняткову роль як засобу соціальної комунікації, все ж не всі вчені вважають мову як систему основою комунікації. Так, засновник біхевіоризму Дж. Вотсон вважав основою комунікації вважав мовні сигнали, маніпулювання якими дає можливість впливати і на людини і на її думку, а отже і на громадську думку, мова про яку більше детально піде у наступному підрозділі [27, с. 72].

Природно, що розвиток засобів комунікації в контексті розвитку високих технологій, якими відрізняється сьогоднішнє суспільство, призводить і до удосконалення існуючих та створення нових типів і моделей комунікації.

Саме тому, останній з вищезгаданих типів комунікації – віртуальна комунікація - є найбільш сучасним і є характерним для сфери масової комунікації і викликає найбільший інтерес з точки зору дослідження, адже в процесі розвитку технологій і виникнення мультимедійних систем сама природа комунікації зазнала серйозних змін. Вже не можна говорити про чіткий розподіл функцій між комунікаторами, бо суб'єкт може представляти ці елементи одночасно за рахунок одночасного і багатоканального доступу до інформаційних систем великої кількості суб'єктів, чим фактично стирається межа між реальністю і віртуальним світом, а ролі суб'єктів є гнучкими і нечіткими.

Відповідно, сьогодні не можна в цьому контексті не говорити про розвиток і поширення масової комунікації. З розвитком соціальної структури змінювалися форми та особливості аудиторії, на яку було спрямовано інформацію. Еволюціонувала і комунікація, перетворюючись в індустріально розвинутих суспільствах в масову комунікацію, яка здійснюється за допомогою технічних засобів поширення інформації.

Як справедливо зазначає В. Різун, для повноцінного визначення поняття «масова комунікація» не можна обмежитися простим додаванням слова «масова» до проаналізованого нами терміну «комунікація» [26, с. 14]. Масова комунікація - систематичне та одночасне поширення однотипних повідомлень у великих аудиторіях з метою інформування та здійснення ідеологічного, політичного, економічного, психологічного, організаційного впливу на думки, оцінки і поведінку людей; вид соціально-культурної діяльності, що відбувається у формі взаємного об'єднання інтелектуальної і емоційної дії, спрямованої на духовний, професійний зв'язок групи людей.

Масова комунікація - це інформація, яка поширюється географічно на велику аудиторію засобами масової інформації (спілкування влади та суспільства) і при цьому виконує такі функції:

1) Інтеграційну – об’єднання у єдине соціокультурне середовище всі суб’єкти цивілізації (індивідуумів, групи людей, суспільство, держави, міжнародні організації);

2) Комунікативну – створення інформаційного середовища трансграничної інтерактивної активності суб’єктів;

3) Геополітичну – формування власних ресурсів і трансформація сприйняття й значущості традиційних ресурсів. Таким чином створюється нове середовище геополітичних відносин і, як наслідок, технологій поєднання інтересів на рівні міжнародних відносин;

4) Соціальну – трансформація склад суспільства і змінює характер внутрішньо-суспільних відносин;

5) Актуалізаційну – створення а рахунок інформаційних технологій можливості для управління масовою свідомістю і впливом на неї, фактичне здійснення необхідної відповідним суб’єктам інформаційної політики [8, с. 158].

Масова комунікація фактично пропонує інформацію не тільки пізнавального, але й виховного характеру, а також її можна розглядати в якості інструменту насаджування або іншим словом, імплантування владою політичних, регіональних та глобальних центрів нових ідей, рішень, нововведень суспільного характеру.

«Процес масової комунікації забезпечується єдиним джерелом (зазвичай комплексним, таким, наприклад, як телевізійна мережа), який передає одну і ту ж інституціолізовану інформацію мільйонам споживачів. Аудиторія часто гетерогенна, тобто характеризується різними демографічними параметрами, і, як правило, невідома для джерела інформації. Web-сайти та інші нові медіа технології, особливо інтерактивне телебачення, вже починають створювати нові виміри масової комунікації, вводячи в нього новий, міжособистісний вимір» [28].

Глобальне поширення засобів масової комунікації надавало переваги окремим технічно розвинутим суспільствам в управлінні розумами сотні мільйонів людей. Усвідомлюючи можливості засобів масової комунікації, відповідно, варто говорити про необхідність та звичайно бажання управління таким важливим ресурсом. Адже за рахунок управління цим ресурсом здійснюється управління соціальними системами – окремими індивідами та суспільствами в цілому з метою задоволення інтересів суб'єкта, який здійснює таке управління (владні структури, окремі індивіди або їх групи). Особливості здійснення такого управління та різні його методи аналізуються автором в наступному підрозділі.

1.3. Роль засобів масової інформації та комунікації в становленні та поведінці соціуму

Людство перейшло в епоху розвитку інформаційного суспільства і отримує таким чином могутній інструмент для об'єднання зусиль з метою одержання нових знань, спрямованих на рішення глобальних проблем, економічного зростання і підвищення життєвого рівня населення.

Разом з тим, розвиток інформації, інформаційних та комунікаційних технологій необхідно розглядати не тільки як перевагу, але як й інструмент для впливу окремих глобальних та регіональних центрів на розвиток суспільства в окремих державах для досягнення матеріальних цілей на регіональному та глобальному рівнях.

В цьому контексті, вплив комунікацій на суспільство видається досить важливим та цікавим питанням для дослідження. Видається цікавим розглянути один із результатів інформаційного прогресу – засоби масової комунікації та інформації (далі – ЗМК, ЗМІ або мас-медіа), оскільки на нашу думку, в сучасному світі вони несуть в собі не тільки прогрес, але й загрозу.

Саме ЗМК, будучи основним постачальником інформації, впливають на формування внутрішньої картини світу людей, своєрідної когнітивно-поведінкової матриці, на основі якої відбувається орієнтація в світі. І в цьому значенні людина інформаційного суспільства не є вільною, оскільки не має змоги самостійно одержувати повні й, головне, достовірні знання про події, що відбуваються.

У XXI ст. людство живе в інформаційному просторі й щохвилини одержує інформацію про навколишній світ з преси, теле- і радіопередач, Інтернету. Засоби масової інформації і комунікації - соціальні інститути (класично поділяються на пресу, радіо, телебачення, Інтернет), що забезпечують збір, обробку та масове поширення інформації. Видається цікавим проаналізувати історію становлення цих ЗМК.

Першим засобом масової інформації була преса. 31 жовтня 1517 р. Мартін Лютер вивісив на дверях Віттенберзької церкви документ, що складався з 95 тез з критикою папства й індульгенцій (прощення гріхів за гроші). У своєму посланні, розміщеному на дверях приходу, він оголосив, що церква не є посередником між Богом і людиною, і Папа не має права відпускати гріхи людей, так як людина рятує свою душу не через церкву, а через віру в Творця. Інформація поширювалася досить повільно і обмежувалася прихожанами церкви. Тоді Мартін Лютер удосконалив друкарський прилад, який дозволив суттєво збільшити наклад своїх тез. Тези богослова привели у майбутньому до зародження протестантської церкви і фактично здійснили революцію друкарства, що дозволило масово поширювати інформацію (тоді це були памфлети на актуальні теми і листки новин). Протягом XIX ст. преса ставала дедалі дешевшою, масово поширювалась. Одночасно скорочувався час між подією та інформуванням публіки про неї, актуалізувалася інформація в пресі.

На початку XX ст. було винайдено радіо, яке виявило недосяжну для преси здатність інтегрувати мешканців географічно та політично

відокремлених територій. Саме завдяки радіо став очевидним ефект одночасної трансляції однієї й тієї ж інформації на широкі верстви населення.

В свою чергу, як зазначає дослідник соціології В. Городяненко, телебачення ще більше розширило можливості ЗМІ, закріпило уявлення про географічний та соціальний простір і можливості його подолання. «Синтезуючи зображення і звук, воно забезпечило користувачам ширші комунікативні можливості, створило недосяжний для інших ЗМІ «ефект присутності», ілюзію безпосередньої участі у важливих політичних та культурних подіях. Завдяки телебаченню соціальний світ став персоніфікованим, унаочненим: люди почали отримувати конкретну інформацію про те, що, де і як відбувається» [29].

Фактично, телебачення створило ілюзію безпосереднього двостороннього спілкування, а систематизованість і акцентованість інформації робить телебачення чи не найвпливовішим ЗМІ сучасності.

Найновітніший ЗМК - Інтернет («всесвітня павутина») — потужна мережа технічних засобів об'єднаних в єдиний інформаційний простір. Він відкриває доступ до будь-яких розміщених в ньому інформаційних баз даних (текстової, аудіо- чи візуальної інформації), надає змогу використовувати їх, обмінюватися даними, вступати в комунікацію з необмеженою кількістю осіб. До системи Інтернет підключені тисячі бібліотек, підприємств, органів управління тощо. Однак, головною рисою Інтернету є високий ступінь незалежності інформаційних пакетів, оскільки вони не цензоруються.

Цікаво відмітити спостереження М. Маклюена щодо деяких сучасних засобів масової інформації, підкреслюючи, що деякі з них вже передають не стільки саме повідомлення, скільки його автора, наприклад, маючи на увазі телебачення. Як зазначає Г. Почепцов, загальність його підходу призвела до розгляду світу як одного глобальної села, єдність якого досягається за рахунок ЗМІ. Як продовжує Г. Почепцов, «Маклюен запропонував дуже цікаве розмежування «гарячих» і «холодних» ЗМІ: гарячі кошти

завантажують орган почуттів повністю, холодні - через недостатню інформаційної визначеності змушують підключатися всі органи чуття. Радіо, з його точки зору, є гарячим засобом, телебачення - холодним, оскільки радіо не викликає такого високого ступеня співучасті аудиторії у своїх передачах, як телебачення. Його роль у тому, щоб створювати звуковий фон або усувати шуми, як у випадку з підлітком, відкрило в радіоприймачі засіб відгородитися від свого оточення. Телебачення не підходить для створення фону. Воно привертає вас, і без цього, що називається, не обійтися» [30, с. 169-170].

Розвиток ЗМІ спричинив зміни в суспільній психології, способи мислення людей. Вплив ЗМІ на громадськість зумовлюється щонайменше двома функціональними завданнями:

1. Донесення інформації про подію.

2. Зміна реальності й управління нею, зміна громадської думки.

В. Городяненко серед функцій ЗМІ виокремлює наступні:

- інформаційна - спрямована на задоволення інформаційних потреб індивідів і соціальних груп щодо різноманітних подій в суспільстві та світі;

- комунікативна - полягає в організації інформаційної взаємодії між різними соціальними верствами населення, а також між громадськістю та джерелом її інформування;

- виховна - пов’язана з формуванням, зміною установок та ціннісних орієнтацій індивідів, заохочуванням аудиторії до пропаганди певного способу життя, з формуванням суспільно значущих рис, засвоєнням соціального досвіду;

- управлінська — виявляє себе в контролі за взаєминами між членами суспільства, а також між ними і системою керівних органів;

- соціальної адаптації та орієнтації - спирається на потреби аудиторії в інформації для орієнтування у соціальних процесах та явищах, адаптації до змін соціальних, політичних, економічних умов життя;

- соціальної ідентифікації - базується на потребі людини відчувати свою спільність із певними соціальними групами, верствами тощо;

- відтворення певного емоційно-психологічного тонусу - спрямована на зняття психологічної напруги тощо.

З появою радіо та телебачення стало простіше здійснювати управління суспільством в окремо взятому соціумі. Завдяки технічному прогресу географія впливу на людину на початку століття розширилась.

Особливого значення інформаційний чинник набув у XX ст. у зв'язку з розвитком та поширенням демократії як форми правління, за якої джерелом влади є не одна особа чи група осіб, а весь народ. Перетворення народу в суб'єкт політики потребує максимально повного та об'єктивного інформування всіх громадян про політичне життя. Так виникла потреба в засобах масової інформації, і далеко не останньою причиною їх розвитку стало політичне життя суспільства.

Мас-медіа є важливим елементои механізму функціонування демократії. В державі з тоталітарним устроєм ЗМІ відіграють другорядну роль і орієнтовані в основному на інформування про події повсякденного характеру.

Водночас, модель сучасної демократії ґрунтується на фундаменті уявлення про людину як раціонально мислячої та відповідально діючої особистості, яка свідомо і компетентно бере участь у прийнятті рішень. В демократичній державі, що ґрунтується на прийнятті рішень більшістю голосів, володіти такими якостями має не одна людина чи привілейована меншість - еліта, а маси, стала більшість населення.

Досягти компетентних політичних суджень більшості громадян неможливо без ЗМІ. Без радіо, телебачення, газет і журналів навіть добре освічена людина не зможе правильно орієнтуватися в складній мозаїці суперечливих суспільних процесів, приймати відповідальні рішення. Засоби масової інформації дозволяють їй вийти за межі вузького горизонту

безпосереднього індивідуального досвіду, роблять видимим весь світ політики. Вільна діяльність ЗМІ є реальною запорукою свободи слова, без якої всі інші права громадян неможливо реалізувати.

У класичному розумінні демократія неможлива без ЗМІ, їх свобода не повинна означати незалежності, відірваності від суспільства і громадян, інтереси і думки яких вони мають висловлювати. В іншому випадку вони перетворюються у засіб політичного впливу, а громадяни позбавляються реальних можливостей публічного самовираження, свободи слова і думки.

Однак, по мірі розвитку суспільства та розвитку інформаційних систем з'явилися технології ненасильницького формування громадської думки шляхом маніпуляції. Відповідно, маніпуляція громадською думкою стає важливим компонентом у засобах масової інформації і комунікації.

Основними методами маніпулювання громадською думкою є методи інформаційного впливу на свідомість, тобто створення інформаційних потоків та управління ними. Спочатку формується потужний потік несистематизованої об'єктивної інформації, потім відстежується реакція адресатів на різні блоки інформації сегментування інформаційного потоку за допомогою таких методів як замовчування, перестановка і залучення авторитетних інформаторів. Після вторинного відстеження реакції на інформацію слідує фальсифікація реальності за допомогою спеціально підібраних цитат і статистики, потім відбувається фабрикація даних статистики і соцопитувань і на закінчення - емоційне підживлення емоційними кліше, фото- та відеоматеріалами.

Однією з поширених технологій маніпулювання громадською думкою є створення стереотипів, що у наукових колах визначається як «стереотипізація» - створення потрібних образів людей, явищ, соціальних груп. На цих технологіях будується не тільки рекламний маркетинг, але й діяльність виборчих кампаній і робота ЗМІ. У випадку з виборчими кампаніями стереотип підганяється під очікування аудиторії, тобто

відбувається формування відповідного іміджу політика чи громадського діяча. Створюється відповідний імідж, в якому головне не те, що є в реальності, а те, що люди хочуть бачити, і в цьому, як зазначає дослідник В. Ліпман, який, власне, і представив концепцію стереотипізації, ніяк не обійтись без ЗМІ в команді з політиками. Роль ЗМІ в першу чергу полягає в створенні «порядку денного» (англ. «agenda setting») для суспільства – події, що «підлягають внесенню в інформаційний простір і тиражуванню серед населення, оскільки неможливо уявити ЗМІ, які б не формували досвід людини в сучасну добу» [26, с., 75-76].

Маніпуляція пов'язана з цілеспрямованим впливом на кого-небудь для досягнення заздалегідь спланованих результатів. Роль і значення маніпуляції стали усвідомлюватися в результаті широкого використання політичних технологій та завдяки вивченню так званого «масового суспільства» та «масової свідомості» [31].

Поширення різних політичних, філософських, наукових, художніх, інших мистецьких ідей з метою їх упровадження у громадську думку та активізацію, тим самим використання цих ідей у масовій практичній діяльності населення, дослідники визначають як пропаганду. Водночас до пропаганди належать повідомлення, які поширюються для здійснення вигідного впливу на громадську думку, провокування запрограмованих емоцій та зміни ставлення або поводження певної групи людей у напрямі, безпосередньо чи опосередковано вигідному організаторам. Усі вищезгадані та інші акти здійснюються не в останню чергу завдяки засобам масової комунікації або інформації.

ЗМІ відіграють фактично ключову роль у впливі на громадську думку, також можуть бути залучені й інші засоби масової комунікації, зокрема соціальні мережі. За даними досліджень, найбільше населення довіряє телебаченню, потім Інтернету, газетам і радіо. Незважаючи на відмінності, всі ЗМІ використовують схожі маніпулятивні прийоми: приховування

інформації, зміщення акцентів, використання авторитетів, відбір поточних подій для повідомлень, повторення, семантичне маніпулювання та ін. в свою чергу, громадська думка формується під впливом масової інформації, що циркулює комунікативними каналами суспільства і подається ЗМІ. У процесі соціальної комунікації важливим моментом є пропагандистський акцент, а поняття пропаганда взагалі є центральним для них.

Суспільне життя потребує опосередкованих форм спілкування та спеціальних засобів комунікації між різними носіями влади, державою та громадянами, суб'єктами політичної, економічної та духовної діяльності.

У сучасному світі роль засобів масової комунікації постійно зростає. ЗМК можуть бути не тільки важливим засобом інформування населення, але вони активно використовуються владою для політичного маніпулювання. Нині вже нікого не здивуєш, назвавши ЗМІ четвертою владою (поряд із законодавчою, виконавчою та судовою). Сьогодні ЗМІ не тільки маніпулюють громадською думкою, але й перетворюються на важелі управління. Легітимізація дій влади, намагання подати їх такими, що підтримуються суспільством, інтегрування широкої аудиторії - усі ці аспекти перебувають у центрі уваги дослідників масової комунікації. Дослідження останніх років свідчать про різке посилення контролю за інформацією з метою управління громадською думкою (с.41). Легітимізація владних дій, створення позитивної громадської думки щодо владних структур, підтримка домінуючих ціннісних орієнтирів у суспільстві - саме цього влада чекає від мас-медіа.

Суспільна свідомість є також частиною процесу комунікації. Отже суспільство, група людей не лише сприймає пропаганду, але й реагує на неї. Слід зауважити, також що аудиторія ЗМІ за інформацією, поглядами, ментальністю взагалі є неоднорідною. Окремі верстви населення та індивіди по-різному реагують на те, що їм повідомляють, чи щось трактують. Отже

некоректно вести мову про масову свідомість при розгляді конкретних випадків функціонування системи масової комунікації:.

Як стверджує переважна більшість дослідників - політика в цивілізованому світі реалізується через демократію, яка фактично не може бути повноцінною без засобів масової інформації. Вважається, що завдяки ЗМІ в суспільстві формується громадська думка, яка притаманна демократичному устрою та є оплотом громадянських прав та свобод кожної людини. На нашу думку, ЗМІ відіграють роль ретранслятора, дзеркала вибудованого політичною елітою іміджу побудованого на сподіваннях суспільства у даному випадку виборців. Між політикою ЗМІ та громадською думкою наявний тісний взаємозв'язок.

В демократичних суспільствах в ЗМІ присутні технології маніпуляцій різних політичних груп, в тоталітарних режимах – монополія держави на маніпуляцію. З теоретичної точки зору, під думкою взагалі розуміють оціночне судження, що виражає ставлення суб'єктів до конкретних об'єктів дійсності. Але як у першому так і другому випадку громадська думка є індикатором суспільних настроїв.

У понятті громадська думка багато визначень. Серед поширених - це складова частина суспільної свідомості, що відображається у міркуваннях і вчинках людей з приводу соціально значимих фактів, проблем, подій та фактів дійсності.

Громадська думка також відображає стан свідомості, який включає в себе явне або приховане ставлення різних соціальних груп до подій, фактів або процесів соціальної дійсності, в тому числі політичної діяльності та фіксує сприйняття дійсності через призму масової свідомості у якій віддзеркалюються як спільні, так і роз'єднуючи інтереси класів, національних, професійних, духовних та інших спільностей.

Які б ми визначення не розглядали, дослідники ідентифікують громадську думку як масову суспільну свідомість, як складне надіндивідуальне утворення, що існує в суспільстві.

Громадська думка з'являється у первісному суспільстві, як вираження колективної думки роду, племені, общини та відігравала регулюючу функцію у відносинах людей.

Можна стверджувати, що суспільна думка здійснює конкретний вплив на суспільну діяльність. Коли вона збігається з об'єктивними потребами розвитку суспільства відбувається прискорення соціального розвитку і як наслідок здійснює позитивний вплив.

У випадку коли громадська думка не збігається із потребами суспільства і є реакційною вона негативно впливає на процеси, що мають місце у суспільстві.

Носіями, суб'єктами громадської думки є суспільство в цілому та різні соціальні спільноти, групи, колективи.

Будь-яка соціальна спільнота складається з окремих індивідів, тому і громадська думка не може сформуватися інакше, як на підставі індивідуальних думок.

Отже можна стверджувати, що громадська думка є станом масової свідомості щодо суспільних подій, до діяльності різних груп, організацій, окремих осіб; висловлює позицію схвалення або засудження з тих чи інших суспільних проблем, регулює поведінку індивідів, соціальних груп і інститутів, насаджує певні норми суспільних відносин; діє як у межах суспільства в цілому, так і в рамках різних соціальних груп.

За допомогою комунікацій і цілеспрямованої систематизованої інформації в суспільстві можливо реалізувати будь-яку ідею. Наприклад, можна змінити сприйняття індивідом або навіть суспільством навколишнього середовища, загальноприйнятих людських цінностей, і навіть світу в цілому. Цей тезис довів у 1990 р. американський соціолог Джозеф Овертон своєю

«теорією вікон».[1] Теорія Дж. Овертона полягає у тому, що будь-яка ідея, навіть безглузда або абсолютно несприйнятлива на перший погляд, може все ж бути сприйнята суспільством. Як доводить вчений, завдяки спеціальній технології можна руйнувати суспільні інститути, створювати та реалізовувати будь-які ідеї, навіть недопустимі з моральної точки зору. Для цього потрібно лише 5 кроків у поєднанні з комплексом інформаційних і комунікаційних технологій.

Для нас такий порядок речей є неймовірним, але в дії «теорію вікон» можна побачити легалізацію в цивілізованій Європі і Західному світі в цілому гомосексуалізму, який все частіше закріплюється на законодавчому рівні.

Також це ми можемо спостерігати на прикладі історичних подій, коли окрема група держав намагається за допомогою підміни історичних фактів змінити трактування Другої світової війни. За допомогою інформаційних технологій через комунікації відбувається переформатування сприйняття історичних подій і їх трактування. Намагання відбілити агресора через порівняння з переможцем у війні. Спочатку істориками наводяться приклади жорстокості системи державного устрою агресора і держави жертви, а потім між ними ставиться знак рівності. Наступним кроком стає намагання представити агресора жертвою (мається на увазі фашистська Німеччина і Радянський Союз).

---

[1] «1-й крок. Від немислимого до радикального»: групою зацікавлених осіб або організацією пропонується для обговорення в наукових, академічних колах неприйнятна для суспільства тема. Наприклад, канібалізм.
«2-й крок. Від радикального до прийнятного»: паралельно з обговоренням теми з'являється група прихованих канібалів, які, як видається, є серед наукових кіл. Засоби масової інформації тиражують цю новину у своїх виданнях. Знімається табу на обговорення теми. Вводиться новий термін.
«3-й крок. Від прийнятного до розумного»: піднімається тема права вибору. Право на різні смаки і вподобання.
«4-й крок. Від розумного до популярного»: тема тиражується у ЗМІ - інтерв'ю, ток-шоу. Виявляється, що серед відомих учених, митців були канібали.
«5-й крок. Від популярного до політики/норми»: багато людей виявилися канібалами, а в низці африканських країн це норма повсякденного життя.

Отже, як випливає з вищезазначеного, дійсно нерідко в ЗМК використовуються маніпулятивні прийоми впливу на свідомість людей, створюючи ілюзію свободи вибору, але насправді обмежуючи свободу самовизначення особи. З цією метою можуть бути застосовані технології прихованого тиску на емоційну складову масової свідомості. Наприклад, фахівцям у сфері пропаганди відомо, що масовий прояв пригніченості на фоні переживання почуття вини, знижує вольовий потенціал суспільства, створюючи передумови для успішного маніпулювання. Залежно від емоцій і почуттів, що переживаються масами, можна підготувати сприятливі умови для непомітного залучення людей у певну діяльність. При цьому більшість людей буде впевнена, що вчинила вчинок добровільно й усвідомлено, без зовнішнього впливу.

Наразі несвідомі психічні процеси грають колосальну роль у життєдіяльності людини. Неусвідомлювані установки здатні впливати на поведінку індивіда, окремих груп сприяти домінуванню певних думок, відчуттів. Сьогодні інтерес до проблеми управління поведінкою людини через її підсвідомість зростає в зв’язку з новими науковими відкриттями про функціонування людського мозку.

Маніпулювання може мати місце лише в тому випадку, якщо об’єкт впливу з самого початку має видимість свободи вибору, можливість здійснення альтернативної дії. Для того, щоб маніпулювати масами, еліти створюють їм ілюзію, видимість свободи і самостійності, активно використовуючи ЗМК.

У всі часи владні еліти прагнули максимально ефективно контролювати масову свідомість. Управління масовими настроями виступала і виступає, перш за все, як засіб досягнення, здійснення й утримання влади, спосіб реалізації економічних, політичних, соціальних, культурних інтересів і задач.

Є дві стратегії управління народами – тоталітаризм та демократія. Тоталітаризм базується на об'єднанні мас шляхом залякування і ідеологічної обробки в організовану, контрольовану і керовану структуру.

У суспільствах демократичного на перший погляд типу, формально населення володіє особистою й політичною свободою, але фактично маніпулювання суспільною свідомістю з боку політичної та економічної еліт перетворює вибір більшості громадян з вільного свідомого рішення у формальний акт, наперед запрограмований фахівцями з формування масової свідомості.

Однією з поширених технологій маніпуляції є технологія «спільної відповідальності», або «поділу відповідальності». Ця технологія притаманна державам з нестійкими політичними режимами, в яких можлива зміна такого владного режиму через внутрішні, а частіше зовнішні чинники, шляхом державного перевороту або революції.

Розглянемо два випадки - помірний та агресивний. У першому, якщо до влади приходить політична еліта після революційних змін з чіткою програмою розвитку, до розбудови держави залучається громадськість на добровольчих засадах. У другому випадку громадськість залучається примусово, в залежності від рівня освіти, для здійснення терору над противниками режиму. Усвідомлюючи злочинність своїх дій разом із можливою відповідальністю, у випадку падіння режим паде, соціум який разом з політичною елітою чинив злочини, продовжує підтримувати режим і вчиняти злочини. У першому і другому випадках широко залучаються ЗМІ, які, у поєднанні з адміністративним ресурсом, є основним ретранслятором психологічного та силового впливу.

Проблема свободи, самовизначення особи в умовах інформаційного й психологічного впливу ЗМК є складною й неоднозначною. Дослідники цієї теми вважають, що жертви маніпуляцій несуть частку відповідальності за прийняття рішень, оскільки часто люди дозволяють собою маніпулювати,

перекладаючи відповідальність за свої вчинки на інших. Невміння, а деколи і небажання критично, осмислено підходити до отриманої інформації, уважно її аналізувати призводять до того, що люди добровільно стають заручниками маніпулятивних технологій.

При цьому, можна не погодитися з цим тезисом оскільки вразливість до маніпуляції залежить від різних факторів від соціального статусу до рівня освіченості. Доведено, що суспільство з низьким соціально-економічним устроєм більш вразливе до технологій маніпулювання ніж розвинуте. Безперечно, на ЗМІ покладена «місія» тримати свідомість аудиторії «під контролем» і з цією метою вони виступають «сурогатами зрілих соціальних ідей», які і пропонуються «сірій масі» (фактично, переважній більшості населення).

Враховуючи вищезазначене, саме така роль ЗМІ, як справедливо зазначає професор А. Чічановський, а з ним, в свою чергу, погоджується і науковець В. Набруско, піддає сумніву неформально відведену для ЗМІ по всьому світі роль «четвертої влади». Насправді, ЗМІ повсякчас узгоджують свою діяльність або з діючою владою або є під контролем суб'єктів, які прагнуть влади і використовують ЗМІ як засіб тиску і досягнення своїх цілей.

Однак, незважаючи на можливості маніпулювання ЗМК кожна людина несе відповідальність за свій вибір. Відповідно, можна говорити про те, що не все, що циркулює каналами ЗМІ, ефективно впливає на суспільство. Дійсно, підтасовуються факти, замовчується правдива інформація, поширюється неправдива інформація, застосовуються прийоми напівправди, фрагментації в потрібному контексті інформації, проте в основному освічені індивіди не піддаються маніпуляції зі сторони ЗМК.

Цікаво відмітити і теорію культивації, що зародилась у рамках дослідницької програми «Проекту культурних індикаторів», яку у 1960-х роках очолював Дж. Гербнер, вчений з університету Пенсільванії. Основне положення цієї гіпотези полягає в тому, що чим більше часу глядач

проводить перед телевізором, тим більше його сприйняття світу наближається до того образу реальності, який він бачить на екрані.

Дослідники, що займаються феноменом культивації, підкреслюють, що між телебаченням або носієм інформації і отримувачем здійснюється динамічна взаємодія. Ступінь культивації глядачами моделей, представлених телебаченням, залежить від ряду факторів. Деякі глядачі більш схильні культиваційному впливу, що пояснюється певними особистісними характеристиками, особливостями соціального середовища, культурними традиціями.

У рамках досліджень доведено, що інтенсивність ефекту культивації, нав'язування думки через культурні, розважальні, новинно-політичні програми, фільми визначається освіченістю глядачів. Чим освіченіший глядач, аудиторія тим нижчий ефект культивації. Отже, культивація ідей через засоби масової інформації і комунікації прямо залежить від рівня освіченості суспільства. В країнах з низьким рівнем освіченості культивації піддається більше суспільства ніж в країнах з високим рівнем освіти.

Отже, технічний прогрес, поява сучасних засобів спілкування та передачі інформації спричинили кардинальні зміни у системі соціального контролю та програмування соціального порядку. Сучасні засоби масової інформації повністю контролюють поширення інформації, що визначає наші уявлення, установки, а в кінцевому результаті і нашу поведінку. Навмисно фабрикуючи повідомлення, які спотворюють реальну соціальну дійсність, вони, без сумніву, з тим чи іншим успіхом намагаються маніпулювати масовою свідомістю. За допомогою інформаційних технологій та засобів масової комунікації можна докорінно переформатовувати прийнятні для сьогоднішнього звичайного представника суспільства цінності.

ЗМІ пропонують нам готові моделі поведінки, надають готові думки та тлумачення, по суті, перетворюючи суспільство у бездумну масу споживачів інформації.За допомогою мас-медіа та соціальних мереж здійснюється

кероване моделювання свідомості суспільства і як результат підпорядкування мас цілям внутрішньодержавній чи глобальній еліті. Як правило, маніпулятори забезпечують широку підтримку такому соціальному строю, який не відповідає істинним довгостроковим інтересам більшості.

Способів маніпуляції багато, але головним є контроль на всіх рівнях над інформаційним простором і генеруванням ідей. Володіти і управляти засобами масової інформації, як і всіма іншими видами власності, можуть лише ті, в чиїх руках капітал. Радіо і телекомпанії, газети, журнали, соціальні мережі належать конкретним корпораціям і державам.

Висновки до розділу 1.

Інформація сьогодні – це навіть більше, ніж спосіб володіти світом. Завдяки прогресивному розвитку інформаційних і комунікаційних технологій створюються умови для ефективного використання знань та інформації для вирішенні найважливіших завдань управління суспільством в межах однієї держави та по всьому світу. Успішний розвиток світової спільноти на чолі з суверенними державами, які стали на шлях постіндустріальної цивілізації розвитку інформаційного суспільства, залежить від інформаційного впливу. Крім того, інформаційна взаємодія різних груп суспільств — найважливіша форма соціальної взаємодії.

Інформаційний чинник в останні роки спричинив революційні зміни. Зараз увесь світ включений в єдину інформаційну систему, причому вона працює фактично в режимі реального часу.

У цьому зв’язку варто виділити масову комунікацію як систематичне та одночасне поширення однотипних повідомлень у великих аудиторіях з метою інформування та здійснення ідеологічного, політичного, економічного, психологічного, організаційного впливу на думки, оцінки і поведінку людей; вид соціально-культурної діяльності, що відбувається у формі взаємного об’єднання інтелектуальної і емоційної дії, спрямованої на духовний, професійний зв’язок групи людей.

Особливого значення на сьогодні набуває здатність ЗМК управляти розумами сотні мільйонів людей внаслідок глобального їх поширення. Усвідомлюючи можливості засобів масової комунікації, відповідно, варто говорити про необхідність та звичайно бажання управління таким важливим ресурсом.

Відповідний розвиток ЗМІ спричинив зміни в суспільній психології, способи мислення людей. Вплив ЗМІ на громадськість зумовлюється такими функціональними завданнями як донесення інформації про подію та зміна реальності й управління нею, зміна громадської думки. З цією метою використовується на практиці маніпуляція (з метою змусити більшість (або меншість) брати участь (або не брати участь) в укоріненні певної практики). Вона є одним з основних засобів соціального контролю та базується насамперед на жорсткому використанні інформаційного апарату і апарату формування ідей.

ЗМІ відіграють фактично ключову роль у впливі на громадську думку. Однак, варто дедалі більшу увагу сьогодні говорити про широке залучення і відповідний вплив інших ЗМК, зокрема, соціальні мережі (в дипломатії навіть набув відповідного поширення термін твітер-дипломатія). Ця платформа для спілкування між абсолютними різними індивідуумами, представниками різних груп населення здатна впливати та проектувати певні зміни в цілому суспільстві та навіть державі (актуальний приклад – координація дій активістів як рушія суспільних перетворень в певних країнах через соціальні мережі).

Отже, не викликає сумнівів і твердження, що за допомогою комунікацій і цілеспрямованої систематизованої інформації в суспільстві можливо реалізувати будь-яку ідею - змінити сприйняття навколишнього середовища, загальноприйнятих людських цінностей, і навіть світу в цілому індивідом або навіть суспільством (вікна Овертона та культивація).

Безперечно, на ЗМІ покладена «місія» тримати свідомість аудиторії «під контролем» і з цією метою вони виступають «сурогатами зрілих соціальних

ідей», які і пропонуються «сірій масі». ЗМІ мають відповідально ставитися до такої влади.

РОЗДІЛ 2
КОМУНІКАЦІЙНІ МОДЕЛІ ВІДОБРАЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДИСКУРСІ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1. Структурні та функціональні параметри інформаційного простору: соціальнокомунікаційний аспект

Як було детально доведено вище, людина завжди перебувала в інформаційному просторі. Ще до появи письма існували наскальні написи, які передавали інформацію від людини до людини. З процесом еволюції були винайдені нові методи передачі необхідних повідомлень. Так чи інакше, передача інформації у просторі завжди мала свою мету.

У більшості сучасних досліджень інформаційний простір інтерпретується гранично схематично – як складова частина простору культури, і, одночасно, як особлива галузь фізичного простору, яка може виокремлюватися за заданими характеристиками (наприклад, за носіями інформації). Під час дослідження інформаційного простору важливо вказати не тільки на спадкоємність етапів її становлення, що відповідають певному рівню розвитку культури, а також на той факт, що в аспекті інформаційного середовища вона розвивається за зразком сховища знань. Інформаційний простір дає змогу «робити суспільним надбанням, доступ до якого практично не обмежений бар'єрами простору і часу, системи знань окремих осіб і колективів. Це ставить перед суспільством фундаментальну культурологічну задачу – інтеграцію знань, що дозволяє використовувати в практичній діяльності весь досвід людства, а не протиставляти одне одному фрагменти знань, що накопичені в різних культурах» [32].

Що стосується історичного аспекту вивчення телекомунікації та інформаційного простору, то вже Д. Белл вважав, що в наступному столітті вирішального значення для усіх сфер життя суспільства вирішальну роль відіграє становлення нового соціального укладу, який базується на глобальних телекомунікаціях. Поняття інформаційного суспільства у його розумінні охоплює минуле і сучасне різних країн, що належать до протилежних політичних систем, однак мають спільно здійснювати перехід до соціальної форми цивілізації XXI століття. Д. Белл виокремив в історії людства три стадії: аграрну, індустріальну та постіндустріальну, а також підкреслив основну роль інтелектуальної технології, що впливає на прийняття керівних (управлінських) рішень. Мета комунікацій за Д. Беллом, полягає в впорядкуванні глобального суспільства. «У сучасному суспільстві мільйони людей щоденно приймають мільярди рішень - політичних, фінансових, соціальних... Будь-який одиночний вибір може бути непередбачуваним, в той же час поведінка спільноти (масового суспільства) окреслюється чітко, як трикутники в геометрії». Таким чином Д. Белл визначив основну роль на його думку інформаційного простору.

Поняття «інформація» вперше в історії вжив Р. Хартлі в 1928 році. Він визначив інформацію як кількість меседжів, які передають через засоби комунікації. Н. Віннер зазначав, що інформація – це позначення змісту, який отримує індивід із зовнішнього світу за допомогою органів відчуття. Радянські дослідники здебільшого користувались здобутками та розробками Віннера. Найбільш чіткими були дослідження О. Колмогорова та В. Глушкова. Перший розмежував поняття «масова інформація» (сукупність повідомлень) та просто «інформація» (організовані дані або повідомлення). В. Глушков працював у сфері масового обслуговування, тому в його теорії були присутні тези про вовну автоматизацію інформації та подальша систематизація управління). Поняття ж «простір» вживали більше у фізиці та природничих науках.

Проте у другій половині 20 століття, в наслідок утворення одної світової системи обміну інформацією та даними, відбулося поєднання понять «інформація» та «простір», яке відображало технологічні, структурні та соціальні особливості діяльності нової системи. С. Ширн і А. Манойло зробили акцент на технологічному аспекті функціонування інформаційного простору. Перший зазначений дослідник користується поняттям «світовий інформаційний простір» та пояснює його зміст через впорядкованість. А. Манойло розглядає інфопростір з боку його протяжності, де він являється сукупністю об'єктів, які вступають у взаємодію, а також сама технологія такої взаємодії.

З точки зору соціокультурного аспекту інфопростір розглянув Ю.Перфільєв, подаючи при цьому Інтернет глобальним інфопростором, що можна дифініціювати одним псевдопростором, який являється певною проекцією реального простору і об'єднує всі мережі між собою [33, с. 8].

О. Карпенко синтезував технологічний та соціокультурний аспекти і розкрив суть інфопростору через технології та соціальну взаємодію. В свою чергу, І. Цикунов та В. Васютіна визначили дане явище через його структуру. Цикунов зазначив, що основною функцією інформаційного простору є поведінка індивідів у суспільстві. До його складу вчений включив наступні процеси: ресурси середовища з зовні, матеріальні та інтелектуальні цінності та науково-технічний прогрес [34].

Щодо синтетичного визначення поняття інфопростору, то він передбачає обґрунтування сутності і змісту суспільства як форми організації спільнот. І. Надольний з цього приводу зазначає, що дане явище є певною формою організації, яка є відмінною від природного світу [35, с. 336-337].

Рух інформації в інформаційному полі здійснюється за допомогою фізичного зв'язку між одержувачем і джерелом інформації, що матеріалізується в інформаційному потоці. Сукупність інформації, що переміщується в інформаційному просторі через канали комунікації, науковці

розглядають як інформаційний потік. Залежно від наявності каналів комунікації інформаційні потоки можуть поширюватися як усередині окремих інфосфер, так і між ними.

Структура інформаційного простору є складною та незвичайною. Як зазначає науковець Т. Затонацька, основними структурними складовими інформаційного простору є ті ж інформаційні поля та інформаційні потоки.

Інформаційне поле - це сукупність усієї зосередженої інформації, безвідносно до її форми і стану, що знаходиться у відриві як від об'єкта відображення, так і від суб'єкта сприйняття.

Рух інформації в інформаційному полі здійснюється за допомогою фізичного зв'язку між одержувачем і джерелом інформації, що матеріалізується в інформаційному потоці.

Інформаційний потік - сукупність інформації, що переміщується в інформаційному просторі через канали комунікації. Інформаційні потоки можуть протікати як усередині окремих інфосфер, так і між ними, залежно від наявності каналів комунікації. Організаційний аспект структури інформаційного простору складають множини баз даних і банків даних, сховищ даних, технологій їх ведення, використання, інформаційних систем, мереж, застосувань, організаційних структур, що функціонують на основі певних принципів і за встановленими правилами, що забезпечують інформаційну взаємодію об'єктів [36].

До складу технологічних та організаційних компонентів інформаційного простору відносять інформаційну інфраструктуру - середовище, яке забезпечує можливість збору, передачі, зберігання, автоматизованої обробки і розповсюдження інформації в суспільстві.

Інформаційна інфраструктура суспільства утворюється сукупністю: інформаційних і телекомунікаційних систем та мереж зв'язку, індустрії засобів інформатизації, телекомунікації і зв'язку; систем формування і забезпечення збереження інформаційних ресурсів; системи забезпечення

доступу до інформаційно-телекомунікаційних систем, мереж зв'язку та інформаційних ресурсів; індустрії інформації та ринку інформаційних послуг; системи підготовки кадрів, проведення наукових досліджень; алгоритмів і програмних засобів, що забезпечують функціонування програмно-апаратних платформ тощо.

Інформаційна інфраструктура суспільства - середовище, яке забезпечує можливість збору, передачі, зберігання, обробки і розповсюдження інформації та відноситься до складу технологічних та організаційних компонентів інформаційного простору. В.Л. Плескач зазначає: «Інформаційна інфраструктура суспільства утворюється сукупністю: інформаційних і телекомунікаційних систем та мереж зв'язку, індустрії засобів інформатизації, телекомунікації і зв'язку; систем формування і забезпечення збереження інформаційних ресурсів; системи забезпечення доступу до інформаційно-телекомунікаційних систем, мереж зв'язку та інформаційних ресурсів; індустрії інформації та ринку інформаційних послуг; системи підготовки кадрів, проведення наукових досліджень; алгоритмів і програмних засобів, що забезпечують функціонування програмно-апаратних платформ тощо»(Інформаційні системи і технології на підприємствах - Плескач В.Л. -

Структура інформаційного простору,). Саме тому слід відмітити складність дослідження інформаційної структури і необхідність виділення більш конкретніших елементів із її загалу.

Термін інформаційна інфраструктура почав широко використовуватися тільки протягом останніх декількох років. Комісія Бангеманн запропонувала десять додатків, які ініціювали роботу в цій сфері в Європейському Союзі: телеробота, дистанційне навчання, університетські і дослідницькі мережі, телематичні послуги для малих і середніх підприємств, управління дорожнім рухом, управління повітряним рухом, мережі медико-санітарної допомоги, електронні конкурсні торги, транс'європейські мережі державного управління та інформаційні магістралі міст. Аналізуючи інформаційну інфраструктуру

сьогодні слід відмітити позитивні напрацювання в країнах Європейського Союзу. Інформаційна інфраструктура стала набагато багатшою та розвинулась в інших напрямках. Такі напрямки чітко окреслені законодавством та захищаються спеціальними органами.

Дослідники В. Л. Плескач, Т. Г. Затонацька виділяють наступні основні функції, що нині виконує інформаційний простір: інтегруюча – об'єднання у просторово-комунікативне і соціокультурне середовище різних видів діяльності (економічна, соціальна, культурна, політична); комунікативна - створюється особливе середовище транскордонної, інтерактивної і мобільної комунікації різних суб'єктів, у рамках якої вони здійснюють інформаційний обмін; актуалізуюча - в інформаційному просторі здійснюється актуалізація інтересів різних суб'єктів діяльності шляхом реалізації ними інформаційної політики; геополітична - формуються власні ресурси і змінюється значущість традиційних ресурсів, створюючи нове середовище геополітичних відносин і конкуренції [37].

Інформаційна сфера є рушієм розвитку постіндустріального суспільства та активно впливає на стан економічної, політичної, оборонної та інших складових національної безпеки. Телекомунікаційні технології у поєднанні з соціальними надають широкі можливості маніпулювання свідомістю особистості, групи людей, суспільства, формування суспільних цінностей та впливу на масову свідомість у світовому масштабі. Мас-медіа перетворилися у могутню зброю – засоби інформаційного тиску та політичного тиску на громадську свідомість.

Питання функціонування національного інформаційного простору регламентується такими законодавчими актами України та Європейського Союзу: Конституцією України 28.06.1996 р. (зі змінами та доповненнями);- Законом України «Про інформацію (нова редакція)» від 02.10.1992 р. із змінами та доповненнями 2015 року; Законом України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р. (зі змінами);

Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 р.; Окінавською хартією глобального інформаційного суспільства від 22.07.2000 р.

Перше, що необхідно зробити під час дослідження інформаційного простору, - виокремити визначення поняття та його розмежування з поняттям інформаційного поля. Під інформаційним простором І. Михайлин розуміє сукупність територій, охоплених засобами масової інформації певної категорії (регіональними, національними, світовими), хоча на нашу думку дане визначення скоріш підходить для державного інформаційного простору. [38].

М. Яковенко ж визначає так: «інформаційний простір можна визначити як домінантну складову сучасного простору культури, що визначає рівень, характер і спрямованість культурного розвитку та зумовлює її провідні елементи: наукові, духовні, естетичні» [39].

Дослідниця Н. Шершньова у статті «Національний інформаційний простір як відкрита система» зазначає, що якісні і кількісні характеристики інформаційних процесів у будь-якій сфері життєдіяльності вимірюються за двома складовими: інформаційно-психологічною та інформаційно-комунікаційною. Різнорідність, розподіленість, багатозв'язність і динамічність джерел загроз, об'єктів ураження і ресурсів захисту значно ускладнюють вирішення проблеми забезпечення інформаційної безпеки як інтегруючої складової національної безпеки. Для зменшення цієї складності далі проведено аналіз і систематизацію інформаційних факторів загроз і захисту, які суттєво впливають на забезпечення інформаційної безпеки в усіх сферах життєдіяльності людини, суспільства і держави [40].

Особливістю структури та функціонування інформаційного простору в сучасному світі є той факт, що інформація накопичується та передається з блискавичною швидкістю. Таку миттєвість розповсюдження їй надають сучасні телекомунікаційні та інформаційні технології. Швидкість та

можливість передачі робить інформацію та її вплив чи не найвпливовішим важелем у суспільстві. Саме тому, інформацію сьогодні називають не інакше, як четвертою силою або гілкою влади.

Інформаційний простір суспільства характеризується унікальними суб'єктами і співтовариствами, що не мають прямих аналогів в інших просторах, серед яких можна назвати віртуальне співтовариство, мережеву організацію, віртуальне підприємство. Інформаційний простір завдяки відсутності меж у своїй віртуальності є інтеграційним механізмом організаційних структур у планетарному масштабі.

(англ. - Information space) це … сфери в сучасному суспільному житті світу, в яких інформаційні комунікації відіграють провідну роль. У цьому значенні поняття інформаційного простору наближається до поняття інформаційного середовища».

У переважній більшості досліджень саме визначення «інформаційного простору» інтерпретується як складова частина простору культури, і, одночасно, як особлива галузь фізичного простору, що виокремлюється за заданими характеристиками (наприклад, за носіями інформації).

Основними компонентами інформаційного простору є: інформаційні ресурси; засоби інформаційної взаємодії; інформаційна інфраструктура [41]. Існують різноманітні підходи до визначення самого поняття інформаційного простору. Так, його розглядають як об'єднаний електронний інформаційний простір, який створюється при використанні електронних мереж. Також інформаційний простір можна вивчати з позиція самого явища і як об'єкт уваги державних спецслужб або поєднання банків даних і баз даних; технологій їх супроводу та використання та інформаційних телекомунікаційних систем, які функціонують на основі загальних принципів

й забезпечують інформаційну взаємодію організацій та громадян, а також задоволення їх інформаційних потреб. Однак, у роботі проаналізовано інший аспект даного поняття а саме інформаційний простір як сферу сучасного суспільного життя світу, в якому інформаційні та соціальні комунікації відіграють провідну роль. У цьому значенні поняття інформаційного простору близьке поняттю інформаційного середовища.

Інформаційний простір є більш ефективним у державах, де він відкритий для суспільства, де втілено реалізацію спільних інтересів громадян, суспільства та держави. Ефективний інформаційний простір держави створюється та розвивається виключно на базі якісної державної соціально-комунікаційної політики, що спрямовує до побудови інформаційного суспільства. Цей розвиток інформаційного простору має базуватись на новітніх інформаційних, комп'ютерних, телекомунікаційних технологіях і технологіях зв'язку, що сприятиме бурхливому розвиткові відкритих інформаційних мереж, насамперед Інтернету і створить нові можливості міжнародного інформаційного обміну на його основі трансформації різноманітних видів людської діяльності. У більшості держав світу побудова інформаційного простору розглядається як фундамент соціально-економічного, політичного та культурного розвитку, а тому вони мають цілеспрямовану державну інформаційну політику. Розвиток телекомунікаційних та інформаційних технологій у державі значно посилює вплив ЗМІ на соціально-політичне й культурне життя людей [42]. Інформаційно-комунікаційний простір сучасного суспільства обумовлює реальну поведінку людини. Таке інформаційне середовище створюється як нова форма культури, у якій комунікація стає лише способом існування людей.

Специфікою соціокультурного підходу до інформаційного простору є виявлення взаємозв'язку засобів масової інформації з трансляцією культурних моделей, що задають соціальну ідентичність індивідів. Суб'єкти

інформаційного простору сприймаються не тільки як реципієнти й інтерпретатори, але й як джерела комунікації. Тому у будь-якій державі світ державна еліта спрямовує усі зусилля на контроль інформаційного суспільства, цілеспрямовано формує власну інформаційну вертикаль, створює навколо себе сприятливий суспільно-політичний дискурс, використовуючи всебічно механізми антикризової комунікації, які виконують превентивну й нейтралізаційну функції стосовно опозиційних інфопотоків [42].

Однією з характеристик інформаційного простору є його «трансісторичність», тобто здатність сполучати покоління людей незалежно від того, чи є вони сучасниками. Дане вивчав Х.-Г. Гадамер, який пише: «Позавчорашні і післязавтрішні слухачі, – відзначає він, – завжди належать до тих, до кого ми звертаємося як сучасники до сучасників. Але де пролягає межа, що відокремлює від нас це «післязавтра» і, отже, що виключає того або іншого читача з кола тих, до кого ми звертаємося? Іншою важливою характеристикою інформаційного простору є, на наш погляд, його культурний динамізм, прояви якого, на думку О. Сєрьогіна, можна спостерігати майже у всіх сферах життєдіяльності [43].

Розглянувши та проаналізувавши праці та концепції вітчизняних, а також закордонних науковців щодо питання структурних та функціональних параметрів інформаційного простору, можна дійти наступних висновків.

Інформаційних простір – досить широке поняття, яке включає в себе безліч аспектів, які при аналізі необхідно враховувати. Тому лише вузьке дослідження вузького аспекту інформаційного простору може бути достовірним та повним. Проте, так як інформаційний простір є частиною культури, що розвивається за зразком знань, то його головною особливістю є те, що він може зробити будь-які системи знань окремих осіб і груп суспільним надбанням не зважаючи на часові та просторові бар`єри. . Це ставить перед суспільством основну культурологічну задачу – інтеграцію

знань, що дозволяє використовувати в практичній діяльності весь досвід людства, а не протиставляти одне одному фрагменти знань, що накопичені в різних культурах.

Однією з особливостей інформаційного простору в контексті соціальної комунікації є той факт, що його можна вивчати і з позиції явища, і як об`єкт уваги державних служб, і як поєднання банків та баз даник, і як технології супроводу та використання інформаційних телекомунікаційних систем.

Тому відштовхуючись від всього вище сказаного, випливає те, що в основному інформаційний простір є сферою сучасного суспільного життя, в якому комунікації відіграють основну роль. Найбільш ефективним він є лише у тих державах, де він є відкритим для людей та відбувається реалізація спільних інтересів – як громадян, так і держави. Проте така ефективність досягається лише за умови продуктивного діалогу між громадянами та владою. Такий діалог можливий лише за умови створення його державою на базі якісної соціально-комунікаційної політики. Цей постійний зв`язок між громадянами та державою є шляхом до розбудови сучасного інформаційного суспільства.

«Трансісторичність» інформаційного простору суттєво вплинула на побудову та розвиток суспільства в планетарному масштабі. Сьогодні соціум має можливість поширити та вплинути інформацією на хід подій не залежно від того, чи відбувається це зараз, чи є джерело інформації сучасником. Правильні канали передачі та необхідна актуальна інформація завжди матиме місце в житті соціуму, не залежно від того як давно автор чи творець інформації чи повідомлення його створив.

Всі вище зазначені структурні особливості, функції та підходи сьогодні створюють існуючий соціум, а соціум та громадянське суспільство без інформаційного простору існувати не може.

2.2 Форми відображення маркерів інформаційної безпеки в медіасередовищі

ЗМІ змінюють не тільки саму інформацію, а й сприйняття та світогляд людини. Як відзначає дослідник О. Дмитровський, ЗМІ є засобом політичного, економічного та інших впливів на свідомість і поведінку людей. Таким чином ЗМІ може впливати і на владні структури, змінюючи моделі їх поведінки та впливаючи на національну безпеку держави [44].

З метою досягнення воєнних, політичних або економічних переваг ЗМІ впливають на психіку й поведінку осіб, політичної еліти та населення загалом, піддаючи загрозі національну безпеку держави загалом. Так, під час висвітлення будь-якої події, достатньо сприйняття 10 % реципієнтами інформації, адже саме еліта суспільства в даному випадку виступає своєрідними «лідерами поглядів», які у подальшому формують громадську думку.

Цільовими аудиторіями можуть виступати:

1. Великі групи.
2. Малі групи (еліта).
3. Особи, що приймають рішення.

Завдання ідентифікації цільових груп вирішується шляхом аналізу: джерела інформації, мови інформаційного повідомлення, часу виходу в ефір (оприлюднення), читацької (глядацької) аудиторії ЗМІ, форми оприлюднення (телебачення, друковані ЗМІ, мережа Інтернет, листівки, біг-борди), особи, які озвучують інформацію. Отже, чим більш розвинутою є інформаційна мережа держави, тим менше можливостей для маніпуляцій, використання інформації на користь якогось одного суб'єкта. У слабко розвинутій мережі існує більше можливостей для її монополізації та подачі інформації у викривленому вигляді.

«Загрози інформаційним ресурсам можна розглядати як випадки природного, технічного або антропогенного характеру, що можуть спричинити небажаний вплив на інформаційну систему, інформацію, що зберігається в ній» [45].

До загроз національним інтересам і національній безпеці в інформаційній сфері можна віднести:

• прояви обмеження свободи слова та доступу громадян до інформації;

• поширення засобами масової інформації культу насильства, жорстокості, порнографії;

• комп'ютерну злочинність та комп'ютерний тероризм;

• розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

• намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Загрози інформаційній безпеці є численними, їх можна класифікувати за різними ознаками. Так, за джерелами походження антропогенного походження - вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення. Такими загрозами виступають, наприклад, ненавмисні (помилковий запуск програми, ненавмисне допущення через недотримання правил безпеки роботи в Інтернеті інсталяції закладок тощо); навмисні (інспіровані), та результат навмисних дій людей (наприклад, навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне зараження вірусами, навмисна дезінформація великої кількості людей тощо).

Загрози інформаційній безпеці постійно змінюються разом із швидкоплинним розвитком інформаційного суспільства. Тому, основне завдання інформаційної безпеки - визначення критеріїв моніторингу причин

та умов, детермінант активізації алгоритмів дестабілізації національної безпеки в інформаційній сфері. Класифікація допомагає наблизитися до розуміння витоків їх формування, а отже і розробляти моделі впливу на них.

Згідно з Законом України „Про основи національної безпеки України" до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що е власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [46].

Доктрина інформаційної безпеки України визначає основні реальні та потенційні загрози інформаційній безпеці України класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері, внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, в екологічній сфері [47].

У Законі України „Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки" загрозами інформаційній безпеці визначено: 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 [48].

У Державному стандарті України „Захист інформації. Технічний захист інформації. Основні положення" ДСТУ 3396.0-96 безпосереднє

формулювання класифікації загроз відсутнє, проте в ньому передбачено можливі шляхи реалізації загроз. Саме вони дають можливість уявити або визначити ймовірні загрози інформаційним відносинам (відносинам щодо збору, обробки й накопичення інформації). В частині 4.1.3 підпункту 4.1 пункту 4 визначено, що загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкційованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів [49].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз. Постанова Кабінету Міністрів України „Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" містить п. 16 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, який визначає, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час

функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [50].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз. Державний стандарт України „Захист інформації. Технічний захист інформації. Терміни та визначення." ДСТУ 3396.2-97 містить ряд термінів пов'язаних з інформаційною безпекою та які мають пряме відношення до класифікації загроз [51].

Так, пункт 5 „Загроза для інформації" містить наступні визначення:

5.1. Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

5.2 Порушення цілісності інформації – спотворення інформації, її руйнування або знищення.

5.3 Блокування інформації – унеможливлення санкціонованого доступу до інформації.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації. Загальний критерій не визначено

При розробці заходів захисту інформації, необхідно враховувати велику кількість різних факторів: інформація може бути представлена на різних технічних носіях Інформація може піддаватися обробці в комп'ютерних системах, передаватися по каналах зв'язку і відображатися різними пристроями, розрізнятися за своєю цінністю. Фактично, інформаційна безпека – постійний процес вдосконалення елементів захисту інформації, що базується на системності, комплексності, безперервності захисту, розумній

достатності, гнучкості управління і застосування, відкритості алгоритмів і механізмів захисту, простоті застосування захисних заходів і засобів.

Можна виокремити різні способи захисту інформації:

- правові (за допомогою законодавчих актів);
- морально-етичні (кодекс поведінки);
- організаційно-адміністративні;
- фізичні;
- апаратно-програмні.

Важливою ознакою є афективність (емоціогенність, стресогенність) інформаційного простору, спричинена тим, що переважна більшість присутніх у ньому аудіовізуальних меседжів (образів) мають не інформаційне, а емоційне навантаження, і апелюють передусім до емоцій реципієнтів інформації. Таким чином, фахівці, які створюють медіатексти, розробляючи технології навіювання й переконання, свідомо апелюють до образного мислення людей, дезактивуючи разом із цим раціональне (критичне) мислення. Таким механізмом користуються журналісти, що створюють новини. Це вочевидь виявляється в журналістському дискурсі, який перенасичений маркерами агресивного, „мілітаристського" змісту: „інформаційна атака", „інформаційна блокада", „інформаційно-психологічна війна", „інформаційні небезпеки (загрози, ризики)", „війна ідеологій", „війна світів", „боротьба за сфери впливу", „протистояння політичних сил", „війна між президентом і урядом", а також словами, що активують негативні емоційні реакції і стани („страх", „стрес", „смерть", „паніка", „тривога", „жах", „катастрофа", „трагедія", „катаклізми", „теракти" тощо). Ці маркери стають невід'ємною складовою соціального середовища, а також проникають у масову свідомість. Тому військові конфлікти, міжетнічна ворожнеча, тероризм, екстремізм, „чужинні" стандарти й ідеології, еротика і порнографія – це теми, які найбільше контролюються органами державної влади, а відповідно і громадськістю. Найбільшу увагу науковців і громадськості

привертає домінування в медіасередовищі аудіовізуальної інформації з елементами жорстокості - медіанасильства [52].

Медіанасильство вивчається як спосіб психологічного тиску на думки та почуття глядачів, підштовхування їх до певної поведінки. На думку С.Г. Кара-Мурзи, з трьох основних форм тиску на людину – фізичного насильства (насильства щодо конкретних індивідів), соціального тиску (насильства, що несе загрозу правам і свободам індивідів і суспільству) і психологічного впливу („промивання мізків", маніпулювання переконаннями, цінностями, почуттями, поведінкою), останній найбільш небезпечний.

За Д. Леонтьєвим навіть стресогенний вплив розглядається як значно конструктивніший, ніж вплив маніпулятивний, який завжди є потенційно деструктивним. На рівні індивіда він призводить до згортання здібностей людини. На рівні соціуму - спричинює інтелектуальний і світоглядний хаос, руйнує норми, традиції і навіть здатність соціальної системи до самоорганізації й самовідтворення, що становить загрозу національній ідентичності і національній безпеці.

Потенційними медіа агресорами є будь-які елементи медіа середовища (медійні образи, месиджі чи тексти), що виступають носіями медіа агресії і потенційно здатні провокувати на агресивні дії. Серед медіа агресорів виокремлюють три групи:

1) образи, месиджі, тексти з елементами агресії, насильства, жорстокості, жахів, які об'єднуються спільною назвою „медіанасильство" (бойовики, триллери, фільми жахів, документальна і новинна хроніка, яка висвітлює війни, військові операції, теракти, катастрофи тощо, кримінальна хроніка, що висвітлює побутові й інші злочини, вбивства, тортури, жорстокість тощо), реаліті-шоу з елементами насильства тощо;

2) образи, месиджі, тексти з елементами відвертої еротики і порнографії, які штучно (в неприродний спосіб і в неприродних умовах, а коли йдеться про дітей, ще й неприродно з огляду на їх дитячий вік);

3) „псевдоінформація”, яка чинить активний і наполегливий психологічний тиск на емоційно-почуттєву сферу, світоглядно-ціннісні настанови, особисту ідентичність, особистий вибір:

а) реклама (активне й агресивне нав’язування споживачам певних, здебільшого некорисних і „чужинних” товарів і послуг);

б) однобічна пропаганда („промивання мізків”, експансія „чужинних” ідей, ідеологій, моделей світу, способу життя і т.п.);

в) реаліті-шоу (що активують неприродні бажання, способи мислення і стилі поведінки); г) квазінаукові інформаційні матеріали;

г) псевдоновини і псевдосенсації тощо.

Пропаганда здатна впливати на масову свідомість, консолідувати її навколо тих чи тих проблем і питань, а з другого (і в цьому її небезпека) – вона може підривати авторитет суспільної ідеології, послаблювати суспільні і соціальні інститути, а отже, становити загрозу політичним режимам і національній безпеці держав.

Особливий тип умовно агресивного медіатексту становлять новини (новинні меседжі). Масштабно оприлюднені і масово поширені, вони утворюють принципово новий тип дискурсу – новинний дискурс. За даними досліджень впливу новинних програм на цільові медіа аудиторії, здійснених Дж. Робінсоном, 53% респондентів дивляться новини рідко і дізнаються про них від інших людей, а серед реципієнтів, які стверджували, що регулярно дивляться теленовини на національних телеканалах, 77% практично ніколи не дивляться їх від початку до кінця. Крім того, за результатами дослідження Т. Ньюмена, більшість телеглядачів дивляться новини неуважно. Опитування, проведені безпосередньо після трансляції новин та інформаційно-політичних програм, показали, що зміст продемонстрованих там сюжетів істотно викривляється і швидко забувається, а в пам’яті залишається лише емоційне враження. Розуміючи чи інтуїтивно здогадуючись, що інформація, означена як теленовини, є скоріше квазі-

новинами, критично налаштовані дорослі глядачі і, відповідно, їхні діти найчастіше шукають альтернативну інформацію в інших джерелах (в Інтернеті, в друкованих ЗМІ). Часто новинні телепрограми викликають у глядачів розчарування (45%), страх (49%), відчуття тривоги (60%) [52].

Потенційну загрозу інформації національній безпеці, питання масової комунікації, пропаганди як впливу на думку індивіда для її трансформації досліджував Г. Д. Лассвелл. Його перші дослідження відбулися після Першої світової війни - праця «Пропаганда союзників у Першій світовій війні» про шляхи маніпулювання громадською думкою. Пізніше, на кінець 40-х рр. XX ст. Г.Д. Лассвелл виділяв чотири основні функції мас-медіа: новини й інформування (виявляються загрози суспільству і його цінностям), редакторська (корелювання реакцій частини суспільства на інформацію), відторгнення (рекреаційна) і соціалізації (передача культурних зразків наступним поколінням). Він досліджував медіа ресурс для використання індивідами. Інші автори визначають функції такі як соціалізуючу функцію мас-медіа, створення громадськості, освітню, функцію критики і контролю [53].

Ніклас Луман вважав, що поняття мас-медіа має тенденцію до розширення. «У подальшому терміном мас-медіа будуть позначатися всі інституції суспільства, які для поширення комунікації використовують технічні засоби розмноження». Він виділяв таку важливу медійну функцію як управління за самоспостереженням за суспільною системою. Н. Луман наголошував, що медіа постійно породжують і переробляють подразники. Наслідком діяльності інформаційного простору він вважав уявлення про світ і суспільство, на які й орієнтується саме суспільство [53, 110].

Відомий сучасний політолог С. Кара-Мурза визначає основні тенденції у маніпулюванні думками громадськості протягом останнього століття і звертає увагу на роль ЗМІ у політичних процесах як головного чинника формування думки. У переважній більшості засоби масової інформації

використовують лише як інструмент маніпулювання широкими верствами населення з боку державних і недержавних структур. І лише чітка стратегія національної безпеки в інформаційній сфері та відокремленість даної сфери і не підконтрольність з боку владних структур може призвести до якісного інформаційного суспільства.

Проблеми впливу слова (друкованого, промовленого) на людину вивчають багато наук – від теорії масової комунікації до соціопсихолінгвістики.

Саме соціальні інститути (державні органи влади, громадські організації, політичні партії та ін.) застосовують механізми впливу на аудиторію для досягнення своєї мети. До таких механізмів належать соціологічні опитування (через пошту, по телефону, на вулиці), поширення рекламної продукції (листівки, інформаційні бюлетені), методи безпосередньої комунікації (збори, зустрічі, мітинги, виступи).

Кожен з цих та інших механізмів знаходить своє відображення у ЗМІ: анкетування через пресу, встановлення громадської думки у прямому ефірі аудіовізуальних мас-медіа з одночасним відтворенням рейтингів і діаграм, і публікації листів, звернень, звітів про інформаційний привід на сторінках газет; і приховані методи „чорного піару”. Для того, щоб подолати бар’єри сприймання, інформація повинна стати відомою і зрозумілою, такою, що вкладається до світоглядної схеми кожного представника громадськості. Засоби масової інформації ведуть постійний аналіз суспільної свідомості населення, вивчаючи громадську думку, активно впливаючи на неї та фактично формуючи її. Однією з визначальних ознак позитивної діяльності ЗМІ є знання своєї аудиторії: соціального, демографічного та інших показників.

В інформаційному суспільстві у період виборів інформаційний простір і його засоби стають найбільш впливовою силою і основним засобом формування громадської думки з конкретних питань. Завдання політики –

ознайомлювати громадськість зі своїми планами і рішеннями. Журналістам потрібні політики як джерело інформації, а політикам потрібні журналісти як канал комунікації, тому вони стають активними учасниками інформаційного суспільства. ЗМІ потрібні також урядам іноземних держав, що таким чином можуть впливати на будь-які рішення усередині наприклад сусідньої країни для формування необхідної для них думки чи сприйняття відповідної інформації [54]. Агресія в медіасередовищі (медіа агресія) постає як психологічний тиск на свідомість реципієнта інформації [55].

На державному рівні маркером інформації є її класифікація,наприклад, в Австралії уряд розділяє усю інформацію на дуже секретну, таємну, конфіденційну, захищену [56]. Задля контролю над державним інформаційним простором, забезпечення інформаційної безпеки держави, нерозповсюдження інформації, що може нанести шкоду цілісності держави при її використанні сторонніми особами створюється відповідна стратегія інформаційної безпеки держави. В цьому контексті створюються відповідні маркери інформації, наприклад конфіденційна чи таємна. Перший «документ», що було зашифровано відомий ще з періоду Античності. Це глиняна табличка, знайдена в Іраку, датована шістнадцятим століттям до нашої ери. На ній гончар відобразив його секретний рецепт написання приголосних і зміну написання слів.

Інформаційна безпека покликана сприяти захисту даних від несанкціонованого доступу, використання, поширення, знищення чи несанкціонованих змін. У переважній більшості країн Європейського Союзу створено розвідувальні служби або відповідні підрозділи розвідувальної служби, що називаються «Чорний кабінет», які відповідають за криптографію та слідкування за поштою та інформацію, що розповсюджується. Інформація - цінний актив, як і матеріальні активи підприємства або держави.

Розрізняють певні теорії сприйняття інформації:

Так, Д. Келлнер вважав ЗМІ (телебачення, газети) вельми конфліктним мас-медіа, в якому конкурують зацікавлення різних фінансово-політичних груп. Учений розглядав загрози в інформаційній сфері як втрату демократії, індивідуальності та свободи. Він запропонував наступні шляхи уникнення погроз: демократичну підзвітність, доступність участі громадян, культурне різноманіття. Також він розглядав ідею легітимації, що полягає у виробленні ідей, які ідеологічно забезпечували б функціонування системи [53].

Разом з тим вже Дж. Мільтон визнав, що частина друкованої продукції може нести загрозу суспільству. Але боротись із цієї загрозою він пропонував за допомогою цензурних обмежень. етичних: «неписані…, не примусові закони доброчесного виховання, релігійної та громадянської культури" [53].

Звертаючи увагу лише на морально-етичні засоби захисту інформації, що проаналізовані вище. Події можуть бути представлені медіа засобами лише через систему вже існуючих стереотипів. Інакше аудиторія чи не зрозуміє суті того, що відбувається, чи витратить на розуміння невиправдано багато зусиль (що, врешті-решт, також відштовхне аудиторію). При цьому медіа відіграє активну роль («В більшості випадків ми не спочатку дивимося, а потім визначаємося, а навпаки — визначаємося, а потім дивимося»). Новина і дійсність («правдива картина»), на думку У. Ліппманна — різні речі. Справа в тім, що під час підготовки новин журналісти користуються стереотипами. Саме з їх допомогою визначаються і категорії новинної цінності та зрозумілості. Отже, У. Ліппманн вважав, що інформаційний простір несе насамперед загрозу самій людині, адже вона живе в «псевдооточенні», яке заміщує реальний світ [53].

Щоб зрозуміти стимули звернення аудиторії до медіа-матеріалів актуально розглянути теорію користі та задоволення (англ. uses & gratification) потреб через мас-медіа. Аудиторії задовольняють свої потреби залежно від їх інтенсивності. Аудиторія намагається знайти способи

найбільш повного задоволення своїх потреб за допомогою медіа-засобів (за А. Маслоу): 1) фізіологічні потреби (їжа, сон, секс); 2) безпекові потреби, 3) потреба спілкування, 4) статусні (авторитет); 5) самоактуалізації (самореалізації). За Д. МакКвейлом: інформація, особистісна ідентичність, інтеграція та соціальна інтеракція, розваги.

Близькими до теорій користі та задоволення є теорії змови і медіазалежності. Прихильники теорії змови вважають, що впливові медіа перебувають у руках зловмисних власників і цілком зорієнтовані на їх інтереси і таким чином впливають на думку суспільства чи певних його частин.

Теорія навчання на моделі полягає у тому, що якщо реципієнт спостерігає за зображенням насильства, пізніше він зможе застосувати цю модель поведінки в реальності. Даний ефект засобів масової інформації може завдати шкоди національній безпеці самої держави, створивши потенціальну загрозу серед її громадян, що можуть під впливом відповідного сюжету застосовувати насильство у межах даної держави. Дану теорію досліджував і активно вивчав Ф. Хайдер [53].

Таким чином, збільшення потоку і спрощення доступу до неї приводить не до вирівнювання інформаційних можливостей людей, а до збільшення інформаційного розриву через різну підготовленість і здатність людей сприймати великі обсяги інформації. Висновок: інформаційна революція посилює інформаційну нерівність.

Крім того, автор вважає за доцільне проаналізувати теорію схем. Згідно з нею реципієнти сприймають повідомлення новин не ізольовано, а відповідно до певної схеми, тобто точки зору, яка часто повідомляється на початку матеріалу і керує його подальшим сприйняттям. Тож можна керувати обробкою інформації, обираючи певний напрям (фрейм). Для ілюстрації цієї теорії зазвичай використовують альтернативу: що краще — врятувати 200 осіб чи 600 осіб, але з вірогідністю 33%. Більшість людей обирає першу

альтернативу, хоча в принципі вони одинакові. Обираючи між вірною смертю 400 людей чи 600 людей з вірогідністю 66 % реципієнти обирають другу альтернативу. Таким чином, сприйняттям новин можна керувати, обираючи перспективу презентації інформації.

Ш. Айенгар и Д. Кіндер на основі свого дослідження зробили кілька висновків: 1) оціночні судження про політиків і електоральні наміри спираються на уявлення щодо компетентності політиків і їх здатності вирішувати актуальні завдання 2) найчастіше повторювані повідомлення посилюють сенсибілізованість аудиторії до цих тем; 3) концентрація уваги на певних проблемах створює у реципієнта враження їхньої особливої актуальності; 4) здатність політиків розв'язувати ці проблеми стає дедалі більш значущою для їх оцінки. Тобто виробляються певні установки, які впливають на електоральні наміри.

Концепція П. Лазарсфельда привела до панування іншої точки зору: мас-медіа мають мінімальний вплив на переконання та вчинки аудиторії, люди роблять самостійні висновки, виходячи зі своїх власних потреб, і звертаються до тих матеріалів медіа, які відповідають їх установкам, ігноруючи матеріали, які їм суперечать. Про обмеженість ролі мас-медіа свідчать і його емпіричні данні. Так, у 1940 р. проти Ф.Д. Рузвельта виступали більшість газет, і він впевнено переміг на президентських виборах. У 1948 р. за Г. Трумена виступали лише 16,2 % щоденних газет (14 % від загального накладу). Незважаючи на це демократ отримав 49,5 % голосів виборців, основна частина населення сприймає інформацію не прямо від мас-медіа, а опосередковано, через людей, які мають авторитет у тому чи іншому питанні. Цих людей називають лідерами думок. Виділяли лідерів думок внаслідок опитування. Було поставлено два запитання: чи намагалися Ви когось останнім часом переконати у своїх політичних поглядах і чи звертались до Вас останнім часом за консультаціями з питань виборів. Якщо людина відповідала «так» на обидва запитання, її вважали лідером думок (з таким ж

соціальним статусом і лідер думок тільки у певній галузі, наприклад, політиці). Виявилось, що лідери думок у сфері політики активно користуються матеріалами мас-медіа і мають більше знань із цього предмету, аніж інші громадяни. Таким чином, лідери думок знаходяться на стику масової та міжособистісної комунікації. Вони виконують функції, з одного боку, посередника між населенням і мас-медіа та інформаційну функцію, з другого боку, функцію посиленого впливу на своїх менш комунікабельних та інтегрованих у соціальні групи співрозмовників. Пізніше, у 1955 р. ці ідеї були об'єднані в теорію двоступеневого потоку комунікації, розроблену під час дослідження в м. Декатурі (штат Іллінойс, США). Виявилось, що лідери - це інтроверти, які активно використовують медіа, які є зразками виконання групових норм [53, с. 60].

Лідерами думок нижчого порядку виступають активні споживачі мас-медійної продукції, оскільки потім вони ретранслюють її у власній соціальній групі та мають завдяки цьому певний соціальний статус.

Вплив на 10 % населення (лідерів думок) дало змогу американцям охопити все населення Близького Сходу під час війни в Персидській затоці. Розроблені методики для визначення лідерів думок. Вони полягають у 1) методі самовизначення (тобто як сама людина оцінює свій вплив). Моментом-ускладненням тут є вірогідність неадекватної самооцінки; 2) соціометричному методі (до кого вони звертаються за порадами); 3) методі ключових інформантів (у групі виділяють інформантів і їх опитують на предмет найвпливовішої людини); 4) об'єктивному методі (вимірюються результати впливу одних членів групи на інших).

Г. Почепцов також досліджував вплив «лідерів думок» на трансформацію думки і виділяє такі характеристики лідерів думок (крім їхньої комунікаційної активності): специфічні характеристики за конкретною областю, вони шукають нову інформацію, їм притаманна зацікавленість, люблять розмовляти, володіють знаннями, впевнені в собі, читають

спеціалізовані мас-медіа. завжди в товаристві, одного віку, одного соціального статусу, відкриті до інформації за межами групи. Взагалі-то лідерів думок 10-15 % від складу соціальної групи, та внаслідок того, що з різних питань лідерами думок є різні люди, лідерами виявляються від третини до половини людей.

Виділяють чотири типи людей відповідно до здатності бути лідерами думок: соціально інтегровані, соціально незалежні, соціально залежні та соціально ізольовані. У 1982 р. американська організація *Roper* виділила параметри, які допомагають визначити лідерів думок: 1) діяльність (за останній рік здійснили три або чотири такі дії: взяли участь у громадських зборах, написали лист депутату, написали листа до газети, допомогли політичній партії, брали участь в мітингу); 2) прибуток (30 % отримують більше 50 тис. дол. на рік, приблизно стільки ж — менше 30); 3) освіта (три четверті відвідували середню школу, 11 % вчились далі); 4) користування мас-медіа (читання, а не перегляд — основний шлях отримання інформації); 5) сімейний статус (як правило, одружені); 6) параметри важливості (надають велике значення престижності (торгової марки), ефективному використанню свого часу); 7) відпочинок (часто-густо населення займається спортом, але більш зацікавлене в мистецтвах; 8) довкілля (більше за інших опікуються екологічними проблемами) [57]. Пізніше теорія багатоступеневого потоку комунікації отримала свій розвиток у теорії дифузії. Д. Робінсон внаслідок досліджень дійшов висновку, що є групи відправників думок і отримувачів думок, ролі яких періодично змінюються і фактично розвінчав теорію П. Лазарсфельда. Крім того, ще в часи дослідження «Вибір народу» П. Лазарсфельд з колегами дійшли висновку, що матеріали медіа не змінюють точки зору, а здатні лише зміцнити наявну. Таким чином, було започатковано теорію посилення чи підкріплення, адже більшість людей у міжособистісному спілкуванні не обговорюють мас-медіа.

Теорію дифузії інновацій розробив у 1962 р. Е. Роджерс [58]. Проаналізувавши матеріали досліджень, він дійшов висновку, що люди приймають нові ідеї, товари, інформацію не одразу, а поступово, за кілька стадій: увага, зацікавлення, оцінка, перевірка, прийняття, підтвердження. Спочатку новацію приймають тільки новатори (близько 2,5 % населення), потім ранні адепти (13,5 %), потім рання більшість (близько 34 %), пізня більшість (стільки ж) і, нарешті, пізні адепти (16 %). Роль медіа тут важлива лише на першій фазі — інформувати новаторів. Інші орієнтуються на своїх лідерів думок. Потім медіа можуть бути майданчиком для дискусій. Тож Е. Роджерс вважав, що лідери думок передають від медіа не інформацію.

Теорія передбачає, що влада має бути сконцентрована в руках еліти, яка стежитиме за дотриманням прав меншин. Ж. Бодійяр вважав, що медіа здатні контролювати аудиторію і власний зміст. Мас-медіа приводить до руйнації соціальних зв'язків і міжособистісної комунікації [53, с. 144].

Отже, новини проходять складний шлях від факту до сприйняття, причому на цьому шляху інформація може мимовільно чи навмисне бути викривленою, а аудиторія отримує викривлену картину реальності. В такому разі медіа-картина світу може значно відрізнятись від реальності.

За даними спеціальних досліджень медіаефіру, агресія і насильство в тих чи інших формах присутні практично у 80% представленої медіапродукції України. До методів прихованого впливу на громадську думку належать: нейролінгвістичне програмування; використання „двадцять п’ятого кадру”; методи асоціацій та стереотипів; інформаційні війни; замовчування чи недомовки та ін. За допомогою цих методів здійснюється маніпулювання свідомістю. До методів явного впливу відносимо пропаганду, використання національної ідеї, соціологічні дослідження та ін.

Важливим елементом впливу на громадську думку є просторово-часовий континуум подачі інформації, а також чергування емоційно забарвлених та нейтральних текстів. Тонально забарвлені матеріали сприймаються

аудиторією краще, ніж офіційна інформація. Причому факти, обрамлені негативом, більшою мірою викликають бажання до дій. Результати проведеного експерименту свідчать, що сприйняття відомостей припиняється, або навіть повністю обмежується після прочитання яскравої, емоційно забарвленої статті. Редакціям слід ураховувати цей факт при макетуванні полос для того, щоб розподілити увагу читача між усіма матеріалами або виділити якийсь конкретний текст (фото) [59].

«Початок нового тисячоліття характеризується глобалізацією світових економічних і політичних процесів, невід'ємною складовою яких є інтенсивне використання досягнень сучасних інформаційних технологій. Після вибору Україною шляху до інтеграції в Європу, яка сьогодні активно розбудовує інформаційне суспільство, гостро постала проблема ефективного забезпечення інформаційної безпеки молодої держави. У сучасному світі інформація є найціннішим та найвартіснішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності і т. ін. Тому Конституцією України визначено забезпечення інформаційної безпеки як одну із найважливіших функцій національної безпеки» [60].

Отже, XXI тисячоліття характеризується глобалізацією усіх світових процесів, а їх невід'ємною складовою виступає активне застоування ноу-хау, досягнень інформаційних технологій і їх розвиток. Після вступу України на шлях до інтеграції в Європу і спрямування усіх зусиль на розбудову інформаційного суспільства, постала проблема ефективного забезпечення інформаційної безпеки України. У сучасному світі інформація є найціннішим

глобальним ресурсом, а ЗМІ виступають основним суб'єктом формування в суспільстві громадської думки про події, що відбуваються в державі та світі. У даному підрозділі автор проаналізував роль масової інформації в формуванні суспільства, позиції певної групи населення.

Так, ЗМІ можуть стати знаряддями масової пропаганди та агітації, за допомогою яких формуватимуть громадську думку, що може призвести до порушення національної безпеки держави. Збільшення потоку і спрощення доступу до інформації приводить не до вирівнювання інформаційних можливостей людей, а до збільшення інформаційного розриву через різну здатність людей сприймати різні обсяги інформації. Таким чином інформаційна революція посилює інформаційну нерівність. Інформаційна безпека як складова національної безпеки на сьогоднішній день виступає чи не найголовнішою складовою, адже лише за допомогою повідомлень у ЗМІ будь-яку державу без превентивних дій з протидії пропаганді можуть втягнути до конфлікту чи війни.

Саме за допомогою інформації можуть ефективніше за будь-яку зброю впливати на населення будь-якої держави зовнішні агресори, адже новини проходять складний шлях від факту до сприйняття, причому на цьому шляху інформація може мимовільно чи навмисне бути викривленою, а аудиторія отримує викривлену картину реальності. В такому разі медіа-картина світу може значно відрізнятись. Тому потрібно досліджувати усі види інформації, можливості захисту інформації, що містить державну таємницю, методи боротьби із пропагандою.

2.3. Соціальнокомунікаційні форми регулювання інформаційного простору

Для того, щоб ґрунтовно розкрити дане питання, слід дати визначення поняття «соціальної комунікації». Соціальна комунікація є відносно новим терміном, який виник протягом останніх десяти років. Хоча слід відзначити, що «нове» поняття означає перегрупування та рекласифікацію його з раніше відомих концепцій соціальної взаємодії, соціальних та комунікаційних навичок.

Все ж явище соціальної комунікації краще розуміти через знання і розуміння визначення соціальної взаємодії і визначення комунікації. Під соціальною взаємодією в соціології розуміється форма соціальної комунікації чи спілкування, що являє собою систему соціальних дій щонайменше двох осіб чи соціальних спільнот, або індивіда і соціальної спільноти. Більше того, соціальна взаємодія — це будь-яка поведінка індивіда чи групи індивідів, що має значення для інших індивідів і груп індивідів чи суспільства в цілому в даний момент і в майбутньому [61].

Згідно І.П. Яковлєва та інших численних дослідників, під комунікацією як наукою слід розуміти сукупність досліджень ролі комунікації в суспільстві, маючи на увазі її розвиток, зміст і структуру комунікаційних процесів.

Наприклад, згідно С. Бориснева, під комунікацією необхідно розуміти соціально обумовлений процес передачі й сприйняття інформації в умовах міжособистісного і масового спілкування по різних каналах за допомогою різних засобів комунікації.

М. Андріанов обмежує розуміння комунікації дослідженнями смислових аспектів соціальної взаємодії.

Виходячи з вище зазначеного можна зробити висновок, що соціальна комунікація через свою різноплановість створює сучасним дослідникам певні

труднощі в процесі наукового обґрунтування соціальнокомунікаційних феноменів. Аналізуючи праці дослідників, слід виділити декілька важливих аспектів. Наприклад, Г.Г. Почепцов вважає, що соціальні комунікації «налаштовані на управління соціальними системами, маючи для цього як короткотривалий (тактичний), так і довготривалий (стратегічний) інструментарій. Освіта, бібліотеки чи наука як стратегічний інструментарій підтримують домінуючі моделі світу, які належать даному виду суспільства» [62].

Декрет Другого Ватиканського собору від 4 грудня 1963 року запропонував таке визначення терміну, що обговорюється: «соціальні комунікації це процес який відбувається серед людей і для людей» [63]. Соціальні комунікації визначають і як зібрання комунікаційних положень. Наприклад, О.М. Холод запропонував визначати соціальні комунікації як «галузь знань, що вивчає організаційно впорядковану систему документів, їх масиви, продукти засобів масової комунікації та інформаційні технології, що забезпечують реалізацію інформаційних процесів і намірів при безпосередній участі членів комунікативного процесу» [64]. Так, В.В. Різун вважає, що «під соціальними комунікаціями необхідно розуміти таку систему суспільної взаємодії, яка включає визначені шляхи, способи, засоби, принципи встановлення і підтримання контактів на основі професійно-технологічної діяльності, що спрямована на розробку, провадження, організацію, удосконалення, модернізацію відносин у суспільстві, які складаються між різними соціальними інститутами, де, з одного боку, у ролі ініціаторів спілкування найчастіше виступають соціально-комунікаційні інститути, служби, а з іншого – організовані спільноти (соціум, соціальні групи) як повноправні учасники соціальної взаємодії» [65].

Саме тому термін «соціальна комунікація» використовується для позначення всіх типів передачі вмісту між відправником та одержувачем, з використанням технології і за допомогою агентів, які не можуть бути

кількісними, адже це процес і дія одночасно. Через велику кількість важливих аспекті та складності структури, вона не може бути повністю визначена в одній фразі і потребує комплексного підходу.

Поєднання понять для вирішення питання щодо форми регулювання інформаційного простору слід також звернути увагу на наступний термін.

Хоч наука в Україні зробила за роки незалежності значні прориви в галузях комунікації та інформації, поняття «інформаційного простору» досі залишається актуальним. Проте в такому випадку слід звернутись до іноземних дослідників, в країнах яких давно існує даний феномен і є невід'ємною частиною практично всіх сфер життя людей. Політолог А. Манойло запропонував наступне визначення, яке найбільше охоплює весь спектр впливу цього поняття: «інформаційний простір - це сукупність суб'єктів інформаційної взаємодії чи впливу; власне інформації, призначеної для використання суб'єктами інформаційної сфери; інформаційної інфраструктури, що забезпечує можливість обміну між суб'єктами; суспільних відносин, котрі формуються як наслідок утворення, передачі, розповсюдження і зберігання інформації, обміну інформацією всередині суспільства» [66].

У центрі інформаційного простору стоїть суб'єкт, який у процесі своєї діяльності створює, накопичує, передає, зберігає інформацію. Таким суб'єктом може бути як людина чи соціальна група, так і компанія чи навіть державний орган - тобто всі, хто використовують можливості сучасних інформаційних технологій [67].

Регулювання створює ліміти, обмеження прав, створює або обмежує обов'язок, або розподіляє відповідальність. Регулювання може приймати різні форми: правові обмеження, оприлюднені державним органом, договірні зобов'язання, які пов'язують багато сторін, саморегулювання галузі, наприклад, через торгова асоціація, соціальне регулювання (наприклад, норми), спільне регулювання, регулювання щодо третіх сторін, сертифікація,

акредитація або регулювання ринку. У своєму правовому регулюванні сенсі можна і слід відрізняти від первинного законодавства (парламентом обраного законодавчого органу) з одного боку і прецедентним правом, з іншого боку [68].

Регулювання інформаційного простору тією чи іншою державою є спробою запобігти спричинення певної шкоди в часово-просторових рамках. Одним словом, не дати можливість впливати інформації на суспільство чи громадян окремої країни.

Якщо ми будемо говорити про правове регулювання інформаційної сфери в Європі, то воно містить в собі основні принципи та норми. Такі складові регулюють права та обов`язки суб`єктів процесу обміну інформацією як в масштабі країни так і в міжнародному.

Є.А. Макаренко в монографії «Європейські комунікації» зазначає, що інформаційний обмін в Європейському Союзі регулюється відповідно до основних принципів міжнародного права: суверенної рівності; невтручання у внутрішні справи держав, заборони застосування сили або загрози силою; дотримання міжнародних зобов'язань, мирного врегулювання міжнародних спорів; непорушності кордонів; загальної поваги до прав людини; співробітництва; виконання міжнародних зобов'язань. Ця сфера регламентується також низкою спеціальних галузевих принципів – правом держав на здійснення чи санкціонування здійснення транскордонного телерадіомовлення; зобов'язанням держав запобігати та припиняти поширення ідей, заборонених міжнародним співтовариством; зобов'язанням держав забезпечити вільний доступ до джерел інформації; правом держав на протидію поширенню на своїй території ідей, які загрожують національній безпеці, громадському порядку, моральному здоров'ю населення, правом держав розвивати інформаційну інфраструктуру задля досягнення своїх політичних, економічних і культурних цілей; зобов'язанням держав запобігати та припиняти неправомірне використання національних

інформаційних ресурсів, масивів інформації для ворожої пропаганди та втручання у внутрішні справи інших держав тощо [69].

Дослідник інформаційного права Г.Л. Віленський повідомляє, що Європейське інформаційне право як комплексна галузь містить загальну й особливу частини. До першої належать норми та принципи, які регулюють загальні положення, форми й методи інформаційної діяльності держав, міжнародних організацій, неурядових інституцій, інших суб'єктів міжнародного права. До другої – конкретні інститути та норми європейського інформаційного права, зв’язок між якими має об’єктивний характер. Це – право масової комунікації, телекомунікацій та зв'язку, кіберпростору та глобальної мережі Інтернет, інформаційної інтелектуальної власності та право інформаційної безпеки [70]. Основними джерелами права споживання, використання та передачі інформації в Європі є:

1. Правила, процедури, директиви, конвенції ЄС і РЄ, резолюції, регламенти, хартії, рішення, програми, статути.

2. Законодавство прийняте в межах країн Союзу.

3. Прецедентні рішенні Європейського суду з прав людини, арбітражні справи,рішення судів країн Європейського Союзу.

4. Норми та принципи, які дотримуються суб`єкти європейського права.

Основним джерелом європейського інформаційного права є міжнародні угоди, при чому, особливе місце займають Європейська культурна конвенція, Європейська конвенція про захист прав людини та основних свобод, Європейська угода про обмін інформацією наукового, освітнього та культурного характеру, а також угоди, які регулюють технічні та професійні моменти роботи з інформацією в Європі.

Основною метою усіх держав світу постає забезпечення національної безпеки, і звісно, інформаційна безпека- один із її основних елементів. Вона досягається саме завдяки контролю та регулюванню інформаційного

простору. Але для того, щоб навчитися контролювати інформацію в своїй країні, необхідно пройти ретельну підготовку.

На прикладі Словаччини можна проаналізувати як Європейський Союз співпрацює зі слабо розвиненими країнами у цій сфері. Поточні пріоритети в контролі над інформаційною сферою обумовлені несприятливою ситуацією в Словаччині, оскільки країна значно відстає від інших держав за рівнем розвитку інформаційного суспільства. Несприятлива ситуація в основному викликана незадовільним виконання завдань, визначених у стратегічних документах, відсутність державної концепції інформаційної безпеки; недосконаліть законодавства, невизначеність компетенції, недостатнього інформування, підтримки з боку компетентних органів та інших факторів.

Виникає питання, як саме підготувати правильну стратегію для країни з низьким розвитком національної безпеки в сфері інформації. Перш за все, необхідно підготувати матеріали, технічні та фінансові ресурси для протидії інцидентам в області безпеки, а також в подальшому формувати спеціалізованої організації по боротьбі з комп'ютерною злочинністю та забезпечити взаємне співробітництво, обмін інформацією та досвідом на національному рівні з посиланнями до загальноєвропейського середовища. Такі установи будуть виконувати завдання, брати участь у виконанні завдань, виробляти план дій і т.д. Також слід нарощувати кадровий потенціал, який в даному випадку буде навчатися за рахунок співпраці з іноземними державами.

Таким чином, маючи стратегію, уряд країни може роздавати компетенції структурам, які будуть працювати у сфері інформаційної безпеки держави.

Також важливою формою протидії небезпеці в інформаційному просторі є належне технічне устаткування, оскільки сьогодні атаки ворогів перемістилися з наземної території в кіберпростір.

Розробки програм, які регулюють інформаційний простір, давно вийшли за рамки держави. Це означає, що програмісти фрі-лансери сьогодні з

радістю напишуть програму, яка, наприклад буде блокувати в рамках національної безпеки та безпеки інформаційного простору певні шкідливі віруси, повідомлення чи інформацію. Такими розробками радо користуються уряди країн для регулювання інфопростору в країні. Для прикладу можна навести інтернет-простір. Уряди часто замовляють програми, які змінюють IP-адреси. Причиною такого замовлення є створення ботів, які пишуть пости, коментарі, повідомлення в інтересах уряду або проти ворогів. Такими програмами сьогодні користуються Україна та Росія в процесі інформаційної війни. До речі, феноменом цієї інформаційної війни є те, що Росія веде її на території України, яка є слабкою в програмному забезпеченні і не може блокувати шкідливу інформацію. Україна, в свою чергу, не має широкого доступу до ЗМІ, в тому числі і Інтернет, в Росії, тому глобальну інформаційну війну вести не може, а лише відбивається від постійних інфоатак.

Феномен Росії в плані форми забезпеченні інформаційної безпеки в країні полягає в наступному. Всі найбільш відомі ЗМІ контролюються державою, тому інформація, яка потрапляє до споживача є фільтрованою. В ефір та Інтернет майже ніколи не потрапляє інформація, яку ми називаємо *правдивою або незручною* для держави та тих, хто управляє країною. Крім жорсткого фільтрування інформації та правильної психологічної подачі, в Росії також регулюють інформаційний простір шляхом законодавства, яке встановлює жорстку цензуру та не дає можливості «не схваленим» повідомленням чи новинам потрапляти до споживачів.

Інформаційна безпека в сучасному світі призначена, перш за все, для захисту конфіденційності, цілісності і доступності даних комп'ютерної системи від тих, хто має ворожі наміри. На прикладі США, одним із основних установ, які займаються регулюванням інформаційного простору в національних інтересах є ЦРУ. Конфіденційність, цілісність і доступність іноді називають тріадою інформаційної безпеки Центрального

Розвідувального Управління. Ця тріада перетворилася в те, що зазвичай називають *The Parkerian hexad*. Вона являє собою набір з шести елементів інформаційної безпеки, запропонованих Донном Б. Паркером у 1998 році. *The Parkerian hexad* додає три додаткові атрибути для трьох класичних атрибутів безпеки тріади ЦРУ (конфіденційність, цілісність, доступність).

Атрибути *The Parkerian hexad* наступні: конфіденційність; контроль;цілісність; дійсність; доступність; корисність.

Ці атрибути інформації є неподільними в тому, що вони не розбиваються на додаткові компоненти. Будь-яке порушення безпеки інформації може бути описана як вплив одного або більше з цих основних ознак інформації.

На рівні держави, популярним та гострим є проблема регулювання інформаційної сфери в рекламі. Проблема полягає в тому, що реклама є досить багатогранною. Реклама може представляти не лише товар, а й речі, які можуть загрожувати національній безпеці, як от дії іншої держави чи лідера, популяризація його політики і нівелювання досягнень уряду власної. Така реклама може продавати так звані «західну» чи «східну» політику непідготованому споживачу. Саме тому особливу увагу приділяють сьогодні законодавству, яке регулює діяльність реклами та друкованих засобів масової інформації. В Україні недавно таким проявом регуляції була заборона використання державного прапору в цілях реклами. Часто рекламна інформація є недостовірною та неправдивою, виробники вживають цифри, які не відповідають дійсності, оприлюднюють факти, які не підтвердились, чим порушують основні права людини. За таку діяльність в нормальному громадянському суспільстві такі виробники мають понести покарання, оскільки своїми діями вони вводять покупців в оману.

Одна з проблем в регулюванні реклами є тягар доведення - регулюючі органи повинні довести, що реклама вводить в оману, або рекламодавці повинні довести що це правда. Прецедентне право в США дає можливість

говорити про те, що саме в цій країні питання реклами завжди поставало досить гостро. Але, не зважаючи на всі прецеденти, в процесі інформування споживача про товар сьогодні виробник зобов`язаний довести, що саме такими властивостями наділений товар, який вони продають. У випадку, якщо інформація не підтверджується, на виробника накладають санкції у вигляді штрафу та позбавлення волі відповідальних осіб. Для доведення властивостей товару та донесення саме правдивої інформації в законодавстві сучасних держав прописані норми, які зобов'язують виробника проводити дослідження та тести, які б виявляли якості та властивості продуктів.

Що стосується ЗМІ, які «продають новини», то в даному випадку вони мають право не розголошувати джерела власної інформації, проте в розвинених країнах у журналістів присутній певний кодекс. Інформація має бути підтвердженою обов`язково. Така норма є корисною не тільки для споживачів інформації, а й для журналістів, оскільки оберігає журналіста від судових позовів та доведення розслідування до вірної точки.

Якщо говорити про більш чітку структуру використання інформаційного простору державою, то слід зазначити наступні положення, які виходять з вище зазначеної інформації. Держава використовує інформаційний простір для комунікації з громадянами та для впливу на суспільну думку. Комунікація досягається за рахунок реакції громадян на певну інформацію. Особливо зрозумілим та таким, що можна проаналізувати є соціальні мережі. Часто певні структури роблять дослідження за допомогою зливання в інфопростір так званих «качок», тобто неправдивої інформації, реакцію на яку важливо знати для побудови державної стратегії в тому чи іншому питанні. Для того, щоб відвернути увагу соціуму від певних питань часто створюють штучні інформаційні приводи, які «роздувають» в ЗМІ, в тому числі і в соціальних мережах. Таким чином держава може контролювати порядок денний. Такий спосіб має і позитивний і негативний аспекти. З

одного боку є можливість не спричиняти соціальної напруги серед населення та запобігти нестабільності, а також звертати увагу на проблеми соціуму, виокремлювати найбільш значущі для швидкої реакції. А з іншого боку, держава відвертає увагу населення від помилок чи «тіньових» дій уряду для того, щоб не спричиняти різкої реакції та критики. Позитивний аспект може проявлятися тільки в демократичних країнах, де налагоджена двостороння комунікація «народ-держава».

Як висновок, слід зазначити, що для регулювання інформаційного простору різні держави та співдружності використовують багато різних методів. Відомі нам лише небагато з них. Перш за все, це законодавче регулювання, яке є чи не основним базисом як для процесу контролю, так і для захисту інформаційних кордонів країни та національних інтересів. Законодавство країни дає можливість узаконити та встановити стратегії інформаційної безпеки суспільства, надати повноваження певним установам, які будуть слідкувати за безпекою інформаційного простору, а також прописати програми, які будуть інформувати суспільство щодо можливих загроз та про їхні права. В залежності від політичної системи в державі, законодавство в цій сфері буде направлене на безпеку приватного життя та основних природних людських прав, як в США. Або ж законодавство буде контролювати своїх громадян шляхом обмежень та фільтрації інформації задля контролю інформаційного простору для того, щоб зберегти існуючий режим.

Важливо також для країни є слідкування за інноваціям для того, щоб контролювати національну безпеку від зовнішніх ворогів, які можуть використовувати нові технології у власних інтересах.

Таким чином, в представленому розділі було визначено, що термін «соціальна комунікація» використовується для позначення всіх типів передачі вмісту між відправником та одержувачем, з використанням

технології і за допомогою агентів, які не можуть бути кількісними, адже це процес і дія одночасно. Через велику кількість важливих аспектів та складності структури, вона не може бути повністю визначена в одній фразі і потребує комплексного підходу.

В процесі регуляції інформаційного простору держава повинна чітко виконувати завдання, які вона перед собою ставить у стратегічних документах. Обов`язково необхідно створити державну концепцію інформаційної безпеки, яка буде враховувати всі особливості країни. Слід звернути увагу також на законодавство, воно має враховувати всі аспекти прояву інформаційної безпеки та легітимізувати діяльність компетентних органів.

Не менш важливим в процесі регулювання та контролю інформаційного простору є інформування громадян, тобто ведення діалогу між державою та суспільством, оскільки такий процес дає можливість уникнути безліч перепон на шляху до позитивних результатів в цій області.

Ключовим в процесі підготовки та реалізації процесу контролю інформаційного простору є наявність технічної бази, оскільки в сучасному світі лише той має контроль, хто має можливість отримувати та відправляти найсвіжішу та найактуальнішу (або просто інформацію, яка має вплив) інформацію найшвидше. В такому полі розглянуто приклад інформаційної війни Росії проти України. Через відсутність інноваційного програмного забезпечення та сучасної технічної бази Росія веде «воєнні інформаційні дії» на нашій території і намагається переконувати саме українців у певних міфах або вигадках. Це відбувається через те, що Україна технологічно слабо розвинута країні і не може контролювати навіть свій власний інформаційний простір. Росія ж, в совою чергу, не лише успішно контролює власний, а й намагається впливати на інфопростори інших країн.

Висновки до розділу 2.

Оскільки загально визнане поняття «інформаційного простору» відсутнє, слід зважати, що одна із його основних характеристик - змога робити суспільним надбанням будь-які системи знань окремих осіб і груп без просторових і часових бар'єрів. Це ставить перед суспільством основну культурологічну задачу – інтеграцію знань, що дозволяє використовувати в практичній діяльності весь досвід людства, а не протиставляти одне одному фрагменти знань, що накопичені в різних культурах.

Інформаційний простір є більш ефективним у державах, де він відкритий для суспільства, де втілено реалізацію спільних інтересів громадян, суспільства та держави. Ефективний інформаційний простір держави створюється та розвивається виключно на базі якісної державної соціально-комункаційної політики, що спрямовує до побудови інформаційного суспільства.

Однією з характеристик інформаційного простору є його «трансісторичність».

Найбільш поширений та актуальний спосіб використання інформації та формування потрібного інформаційного середовища у соціальнокомунікаційному вимірі є залучення «лідерів думок». Саме вони достатньо сильно впливають на трансформацію думки, особливо у сфері політики. Вони активно користуються матеріалами мас-медіа і мають більше знань із цього предмету, аніж інші громадяни. Таким чином, лідери думок знаходяться на стику масової та міжособистісної комунікації.

Новини проходять складний шлях від факту до сприйняття, причому на цьому шляху інформація може мимовільно чи навмисне бути викривленою, а аудиторія отримує викривлену картину реальності. В такому разі медіа-картина світу може значно відрізнятись від реальності.

Термін «соціальна комунікація» є комплексним і використовується для позначення всіх типів передачі змісту між відправником та одержувачем, з

використанням технології і за допомогою агентів, які не можуть бути кількісними, адже це процес і дія одночасно.

Метою усіх держав світу насамперед виступає національна безпека, що включає в себе інформаційну безпеку. Вона досягається саме завдяки контролю та регулюванню інформаційного простору. Чим більш розвинена держава, тим більше уваги вона на сьогодні приділяє забезпеченню власної інформаційної безпеки (держава концентрується забезпечення такої безпеки на нормативно-правовому та на виконавчому рівнях, а також відповідно працює з населенням).

Як відомо, сьогодні відносини між Україною та Росією вкрай складні. Щонайменше, дві країни перебувають у стані інформаційної війни (Росія веде її на території України, яка є слабкою в програмному забезпеченні і не може блокувати шкідливу інформацію. Україна, в свою чергу, не має широкого доступу до ЗМІ, в тому числі і Інтернет, в Росії, тому глобальну інформаційну війну вести не може, а лише відбивається від постійних інфоатак.

РОЗДІЛ 3
ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

3.1. Соціальнокомунікаційний зріз загроз національним інтересам у інформаційній сфері

Для того, щоб дати відповіді на значущі питання розділу, перш за все необхідно проаналізувати ключові поняття, без яких не можливо побудувати цілісної картини розуміння соціальнокомунікаційного зрізу існуючих небезпек для національних інтересів.

В цьому випадку розгляд питання слід розпочати із визначення одного із основних понять, які концентрують нашу увагу. Таким поняттям в даному розділі є «інформаційна сфера». Причиною цього є той факт, що на сучасному етапі розвитку суспільства та комунікацій дана сфери відіграє важливу роль. Визначення поняття «сфера» у словнику подано (від грец. sphaira – шар) – це область дій, межа поширення чого-небудь (наприклад, сфера впливу); суспільне оточення, середовище, умови.

Вітчизняна дослідниця інформаційної сфери І.В. Арістова зазначає, що безумовно, за сьогоднішніх реалій інформаційна сфера розглядається і як відносно самостійна сфера, і як допоміжна стосовно інших видів діяльності, адже обслуговує практично усі сфери суспільства (економіка, політика, управління, наука, культура, побут, сім'я). Однак, як в першому, так і в другому випадку мається на увазі вузьке тлумачення поняття «інформаційна сфера». Існуюча політика держави в інформаційній сфері (вузьке тлумачення) спрямована на розвиток безпосередньо інформаційної сфери і на підвищення ефективності розвитку державності, безпеки, оборони, пріоритетних галузей економіки, інших сфер суспільства, міжнародного співробітництва за допомогою інформаційної сфери [72].

Загалом, слід зазначити, що інформаційна сфера в процесі еволюції нарощувала масив знань та показників, саме тому єдиного і точного визначення даного поняття немає. Наприклад, російські дослідники Бачило І.Л., Лопатин В.Н., Федотов М.А. використовують визначення поняття «інформаційна сфера» із законодавства Російської Федерації, а саме під нею в законодавстві розуміється «сфера діяльності суб'єктів, пов'язана із створенням, перетворенням і споживанням інформації» [73]. Західні дослідники зазвичай використовують поняття «інфосфери», що є, по-суті і змісту неологізмом, який складається з двох слів – інформація і сфера.

Перше документальне використання слова «інфосфера» мало місце у 1971 році в *Time Magazine* в огляді книги Р.З. Шеппарда, в якому він пише: «Так як риба не може осмислити воду або птахи повітря, так людина ледве розуміє свою інфосферу, як навколишній шар електронного та типографського смогу, що складається з кліше, журналістики, розваг, реклами і уряду» [74].

У 1980 році поняття було використане Тоффлером в своїй книзі «Третя хвиля», в якій він пише «Чітким і ясним є той факт, що ми віримо в те, що кардинально змінюємо інфосфери ... щоразу ми додаємо цілий новий шари зв'язку в соціальну систему, тому виникає Третя хвиля інфосфери, в якій домінують ЗМІ, поштове відділення» [75]. Визначення Тоффлера виявилися пророчими, як використання «інфосфері» в 1990-х роках за рамками ЗМІ, що почали спекулювати довкола еволюції Інтернету, суспільства і культури.

У своїй книзі «Цифровий Дхарма», пише Стівен Ведро, «Виникаючі від того, що французький філософ-священик Тейяр де Шарден назвав загальну ноосферу колективного людського мислення, винаходу та духовного пошуку, інфосфері іноді використовується, щоб осмислити поле, яке поглинає наше фізичне, психічні та ефірне тіла, вона впливає на наше сновидіння і культурного життя наш розвивається нервова система була розширена, а засоби масової інформації шавлії Маршалл Маклюен передбачив на початку 1960-х, в глобальну обійми».

Термін також використовується Флориди, на підставі біосфери, щоб позначити все інформаційне середовище, створення всіх інформаційних сутностей (таким числі інформаційних агентів, а), їх властивості взаємодій, процесів і взаємин. Це в середовищі порівнянна з, але відрізняється від кіберпростору (який є лише одним з його субрегіонів, як це було), так як він також включає в автономному режимі і аналог простору інформації. Згідно Флориди, можна прирівняти *InfoSphere* до сукупності Буття. Це рівняння приводить його до інформаційної онтології.

Питання механізмів обміну інформацією між державою і суспільством та між суспільством і приватними мас-медіа для України в останні роки є актуальними. Мова йде про необхідність запровадження єдиної концепції державної пропаганди та посилення державного контролю за інформаційним обігом, повернення державі можливостей достатнього інформування суспільства про свої цілі та наміри [76]. Сьогодні для України існують такі потенційні загрози в інформаційній сфері, а відтак, і реальні загрози позитивному іміджу країни: незбалансованість державної політики та від сутність необхідної інфраструктури в інформаційній сфері; зволікання зі входженням України до світового інформаційного ринку; відсутність у міжнародного співтовариства об'єктивного уявлення про Україну; інформаційні атаки й експансія з боку інших держав; витік інформації, що містить державну таємницю, та конфіденційну інформацію, що є власністю держави [77].

Національна безпека кожної держави у сучасному світі більш за все спрямована на протидію інформаційним атакам і загрозам будь-яким в інформаційній сфері, адже це рушій і економіки, і політики і усіх сфер суспільного життя. Світ стоїть на порозі побудови глобального інформаційного суспільства, завдячуючи інтенсивному розвитку інформаційних і комунікаційних технологій та їх широкому застосуванню у всіх сферах людської діяльності. Глобальна інформаційна інфраструктура

забезпечує безпрецедентні можливості для спілкування між людьми, їх соціалізації та доступу до інформації. Особи, суспільства і держави залежать від стабільності і надійності інформаційної інфраструктури, що і може виступати як основна загроза національним інтересам держави.

ІКТ це принципово новий і ефективний засіб, щоб зруйнувати або знищити галузь тієї чи іншої країни, її економіки, соціальної інфраструктури і державного управління. ІКТ мають потенціал, щоб стати засобом боротьби, здатний досягти цілей, пов'язаних з вирішенням чи ескалацією міждержавних конфліктів. Таким чином, ІКТ у сучасних реаліях має характеристики зброї «призначеної для ураження противника в бою», а потенціал руйнівної сили даної «інформаційної зброї» буде зростати в міру розвитку ІКТ і інформаційної інфраструктури суспільства. Найчастіше «інформаційну зброю» використовують у військових цілях як пропаганду та контрпропаганду. Ці проблеми не є новими, і не обмежуються лише однієї країною або регіоном, дана сфера стосується усього світу. Відтепер за допомогою інформаційних повідомлень можна впливати на стан розвитку економіки країни наприклад на іншому континенті. За допомогою інформаційних технологій держави можуть розпочинати війни, що є більш дешевими та не потребують цілих армій. Стратегічна безпека держави полягає у підготовці і превентивних діях щодо попередження негативних наслідків інформаційно-технологічної революції.

Однією з найбільш застосовуваних дій і водночас загроз національній безпеці держави виступає кібертероризм як ефективний засіб впливу на психіку. У загальному контексті інформаційної війни і створення інформаційної зброї проблема вивчення їх психологічного впливу стає важливим питанням. Вплив за допомогою інформації на людей, що приймають рішення, ґрунтуючись на конкретній інформації в сьогоднішній реальності стає пріоритетним об’єктом інформаційно-психологічного впливу

в інформаційній війні. Найбільш традиційною і потужною інформаційною зброєю є пропаганда.

Серед факторів, які сприяють використанню інформаційної зброї і відрізняють її від інших засобів ведення війни визначають:

1) Вільний доступ до інформаційних систем (розвиток інформаційних мереж, швидке зростання і зростаюча складність інформаційної інфраструктури призводить до виникнення глобальної інформаційної інфраструктури з багатьма розгалуженим інформаційними мережами. Люди можуть бути схильні до впливу з різних джерел інформації і таким чином піддаватись кібератакам: думки, статті кваліфікованих осіб, експертів, недержавних суб'єктів, таких як міжнародні злочинні організації, а також з боку з боку добре підготовлених фахівців для ведення бойових дій в кіберпросторі інших держав;

2) Розмивання традиційних кордонів (в першу чергу, розмиття чітких географічних меж, традиційно пов'язаних з національною безпекою, на відміну від ефектів, пов'язаних з втратою державного контролю над поточними глобальними фінансовими і валютними ринками, зміцнення зв'язків національних інформаційних структур і глобального кіберпростору неминуче підриває національний суверенітет держав. Одним з найбільш серйозних аспектів феномену "розмитості державних кордонів" стає неможливість визначити чіткі критерії для розрізнення внутрішніх і зовнішніх джерел загрози національній безпеці.

3) Можливість контролювати сприйняття (факти конкретної події можуть бути суттєво викривлені методами текстових, голосових і відео інформацій. Такі методики можуть дозволить реалізувати комплекс управління процесом суспільного сприйняття або організувати великі кампанії, щоб підірвати довіру громадськості до певних напрямків державної політики, що проводить уряд чи офіційні представники влади. Кампанії такого роду створюють серйозні проблеми не тільки уряду, але і засобам масової інформації, що

подають дану недостовірну інформацію як правдиву і перестають бути джерелом об'єктивної інформації, втрачаючи власні рейтинги та глядачів.

Термін кібертероризм, як правило, відноситься до дій в дезорганізації інформаційних систем, які створюють загрозу життю людей, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків, якщо вони зроблені з метою порушення громадської безпеки, залякування населення або впливу на рішення влади, а також погрози вчинення таких актів [78].

Агентство національної безпеки США, що має доступ до запису телефонних розмов та Інтернет-даних створено виключно для боротьби з тероризмом і серйозними злочинами, однак відповідно до документів, оприлюднених Сноуденом, моніторинг здійснюється за усіма громадянами. Межа між захистом національної безпеки в інформаційній сфері і шпигунством як методом отримання інформації від посадових осіб інших держав виявляється дуже тонка. До того ж, працівника ЦРУ Сноудена визнано терористом по відношенню до США, адже розповсюдження цієї таємної інформації і документів, переданих ним у червні 2013 року газеті *The Guardian* кваліфіковано як терористичний акт проти національної безпеки США. Однак, оприлюднені документи підтверджують використання інформаційних технологій для перехоплення комунікацій високопосадовців не лише США, а й інших делегацій G20.

У сфері інформації у згаданій вище справі використано такі методи, що можуть у подальшому трактуватись як загрози національній безпеці держави, які можна попередити:

• Налаштування Інтернет-кафе, де використовували програму електронної пошти перехоплення і програмне забезпечення - ключ ведення журналу, щоб отримувати інформацію при користуванні делегатами комп'ютерами;

• Проникаючі безпеки на BlackBerrys делегатів, щоб контролювати повідомлення електронної пошти і телефонних дзвінків;

В результаті застосування даних методів можна було дізнатись будь-яку інформацію, наприклад політику та плани турецького міністра фінансів.

Загрозу становило у переважній більшості розкриття інформації, що містилась на технічних пристроях - комп'ютерах та телефонах делегатів. Для досягнення поставленої мети, як подано у документах, поширених Сноуденом, використано технологію «активного збору з поштової скриньки інформації, програмою, що копіює поштові повідомлення, не видаляючи їх з віддаленого сервера», фактично це означає «читання електронної пошти людей, перш ніж вони це роблять» [79].

Основною ж формою кібертероризму залишається інформаційна атака на комп'ютерну інформацію, комп'ютерні системи, обладнання передачі даних, а також інші компоненти інформаційної інфраструктури, що здійснюються окремими особами або групами. Ця атака дозволяє йому проникнути в цільову систему для перехоплення контролю або придушення засобів мережі обміну інформацією, виконувати інші деструктивні дії.

Таким чином, найбільшою загрозою і небезпекою в інформаційній сфері є кібертероризм, за допомогою якого можна отримувати таємну інформацію пов’язану із забезпеченням національної безпеки держави (наприклад, таку, якою володіє розвідка й інші правоохоронні органи) та її використання для досягнення деструктивних для цієї держави цілей, що може призвести до війн, економічних криз, краху банківської системи. Основні дії по забезпеченню і попередженню кібертероризму полягають у забезпеченні інформаційної безпеки, шляхом створення відповідних органів із захисту інформації на рівні держави (у більшості країн світу вони вже існують), розкриттю та виявленню кібер-терористів, створення програмного забезпечення що знаходить технічні засоби атаки в інформаційній сфері.

Національному інформаційному простору держави може загрожувати новий вид війни, а саме інформаційна війна. Проблема захисту національного інформаційного простору від атаки противника полягає в

тому, що він є невидимим, тому боротьба носить специфічний характер. Для повного та детального розуміння організації, методів та засобів захисту національного інформаційного простору, необхідно зрозуміти що таке інформаційна війна.

Поняття інформаційного простору було ґрунтовно досліджено у попередніх розділах, тим не менш, слід нагадати, що інформаційний простір – це сфера в сучасному суспільному житті світу, в якій інформаційні комунікації відіграють провідну роль. У цьому значенні поняття інформаційного простору близьке, але не тотожне поняттю інформаційного середовища. Поняття ж інформаційного суверенітету необхідно ретельно розглянути та проаналізувати. Перш за все, слід звернутись до українського законодавства. В Законі України «Про інформаційний суверенітет та інформаційну безпеку України» говориться наступне:

«Інформаційний суверенітет України - це право держави на формування і здійснення національної інформаційної політики відповідно до Конституції і законодавства України, міжнародного права в національному інформаційному просторі України.

Здійснення інформаційного суверенітету України включає:

- законодавче визначення та забезпечення державою стратегічних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики;

- визначення норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів в національному інформаційному просторі України;

- формування та захист інтересів України в світовому інформаційному просторі, міжнародних інформаційних відносинах; гарантування інформаційної безпеки України»

Б.А. Кормич пропонує наступне визначення: «інформаційний суверенітет — володіння і розпорядження національними інформаційними ресурсами, які включають усю належну державі інформаційну інфраструктуру, інформацію-

незалежно від змісту, форми, часу і місця її створення. І забезпечується виключним правом держави на формування і здійснення національної інформаційної політики, власності на інформаційні ресурси, сформовані за державний кошт, створенням національних систем інформації, встановленням режиму доступу інших держав до інформаційних ресурсів України» [80].

З метою узагальнення існуючих наукових поглядів щодо класифікації загроз інформаційній безпеці та визначення концептуального підходу до формулювання цього елементу правовідносин, пропонуємо розглянути окремі з них. Професор В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці: за джерелами походження: природного походження, техногенного походження, антропогенного походження; за ступенем гіпотетичної шкоди: загроза та небезпека; за повторюваністю вчинення: повторювані та продовжувані; за сферами походження: екзогенні та ендогенні; за ймовірністю реалізації: вірогідні, неможливі, випадкові; за рівнем детермінізму: закономірні та випадкові; за значенням: допустимі та неприпустимі; за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об'єктивні та суб'єктивні; за об'єктом впливу - особа; суспільство; держава. Схожі погляди на перелік загроз інформаційній безпеці висловлює: А. Логінов у власному дисертаційному дослідженні. Зокрема вчений визначає загрози як: – розкриття інформаційних ресурсів; – порушення цілісності інформаційних ресурсів; – збій у роботі обладнання [81].

Б. Кузьменко та О. Чайковська пропонують наступну класифікацію загроз на основі визначення властивостей інформації: – загрози порушення конфіденційності інформації, в результаті реалізації яких інформація стає доступною суб'єкту, що не володіє повноваженнями для ознайомлення з нею; – загрози порушення цілісності інформації, до яких відноситься будь-

яке зловмисне спотворення інформації, оброблюваної з використанням автоматизованих систем; – загрози порушення доступності інформації, що виникають в тих випадках, коли доступ до деякого ресурсу автоматизованих систем для легальних користувачів блокується [82, с. 6–7]. В свою чергу С. Гуцу [83] та О. Литвиненко [84], вважають, що основні загрози інформаційній безпеці можна представити таким чином: – загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; – загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання); – загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову). Л. Євдоченко формуючи власний підхід до класифікації інформаційних загроз визначає і класифікує загрози за кількома критеріями: за способом впливу на об’єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні) [85].

У цьому контексті варто приділити увагу поняттю «інформаційний суверенітет» держави. Інформаційний суверенітет – це та частина державного суверенітету, яка пов'язана з інформацією. Якщо державний суверенітет є «останньою інстанцією» у прийнятті рішень в підтримці порядку, то інформаційний є останнім рівнем в питаннях інформаційної політики, збереженні інформації в межах держави. В зовнішньополітичному плані інформаційний суверенітет належить до повної юридичної рівності з іншими державами і свободі від будь-якого зовнішнього контролю щодо виробництва та використання інформації. Слід також наголосити, що втручання до інформаційного простору та посягання на інформаційний

суверенітет з боку інших держав є одним із проявів інформаційної війни. Зброя сьогодні вийшла на новий рівень і тільки словом та інформацією сьогодні можна нанести набагато більшої шкоди, ніж танком та автоматом. Саме тому інформаційний суверенітет та простір потребують особливої уваги та захисту від інформаційної війни.

Раніше методи боротьби з інформаційною війною були досить репресивними. Достатньо було відібрати радіо або заглушити радіосигнал. Однак, що сьогодні собою являє ця зброя інформаційної війни? Для того, щоб відповісти на це питання, ми розглянемо кожен з методів і дамо короткий огляд найбільш поширених видів зброї, які використовуються для їх досягнення.

Цікаво відзначити введення терміну «мережа» до воєнної лексики. Протягом сотень років, військові зробили ставку на ієрархії, а не мережі, щоб поширювати інформацію. Цивільний прогрес в області комунікаційних технологій слідували мережевим парадигмам, які мають потенціал для серйозних змін у військових колах. Перехід на мережеві структури може зажадати деякої децентралізації управління і контролю. Але децентралізація є лише частиною загальної картини. Нова технологія може також забезпечити широкий огляд, розуміння загальної картини, що підвищує ефективність управління. З цього ми можемо бачити, що навіть, здавалося б, основна зміна в технології для транспортування інформації має потенціал, щоб зробити інформаційний вік війни зовсім іншим.

Одним з найбільш широко узгоджених аспектів інформаційної війни є необхідність звести до мінімуму кількість інформації, до якої ваш опонент має доступ. Велика частина цього захищає інформацію, яку ви приховуєте від захоплення іншою стороною. Зброя, яку використовують для забезпечення безпеки вашої інформації діляться на два класи. По-перше, це ті технології, які фізично захищають сховища даних, комп'ютери і транспортні механізми, в тому числі бомби та куленепробивні корпуси і механізми

запобігання вторгнень, такі як замки і відбитки пальців. По-друге, і, можливо, більш важливо, це технології, які перехоплюються противником. Це, безумовно, включає в себе основні технології комп'ютерної безпеки, такі як паролі, а також більш складні технології, такі як шифрування. Як зазначає Лібікі, «шифруючи свої повідомлення і розшифровуючи чужі, кожна сторона виконує квінтесенцію актів інформаційної війни, захищаючи своє уявлення про реальність» [86].

Маніпуляції інформацією в контексті інформаційної війни є зміна інформації з наміром спотворити уявлення суперника про реальність. Це може бути зроблено за допомогою низки технологій, включаючи комп'ютерне програмне забезпечення для редагування тексту, графіки, відео, аудіо, і інша інформація. Проектування керуючих даних зазвичай робиться вручну; ті, у кого в команді є контроль над інформацією, картину будуть представляти до супротивника, але вищезгадані технології широко використовуються, щоб зробити процес фізичної маніпуляції швидше, як тільки вміст було вирішено.

Остаточні аспекти інформаційної війни - порушення, деградація і відмова. Усі три методи є засобами тієї ж загальної мети - не дати ворогу отримати повну, правильну інформацію. Через їх схожість, багато хто ту ж саму зброю використовує для досягнення однієї або більше цілей. Деякі з найбільш популярних видів зброї, які використовуються для ведення такого роду інформаційної війни є підміни, введення шуму, перешкод і перевантаження [86]. Підміна - це метод, який використовується для погіршення якості інформації, що направляється до супротивника. Потік інформації противника порушується введенням обману або підробленням повідомлення в цьому потоці. Метод працює, тому що це дозволяє забезпечити «неправдиву інформацію для системи збору конкурентів, щоб спонукати цю організацію зробити неправильні рішення, засновані на цій помилковій інформації» [87].

Ще один спосіб зашкодити в отриманні правдивої інформації, яку шукає опонент, внести шуми. Фоновий шум ускладнює процес противнику, оскільки йому важко відокремити реальне повідомлення від шуму. Це особливо корисний метод, якщо противник використовує форми бездротового зв'язку. Крім того, існує метод перешкоди та метод перевантаження.

Також існують протидії вище наведеним прикладам інформаційних атак, наприклад, щоб захиститися від атак збору інформації ворогами про нас і про конфліктну ситуацію. Робота на цьому напрямку включає в себе захист власної інформації від перехоплення і запобігання потрапляння інформацію в пункти збору противника. Доступні контрзаходи для захисту від збору інформації, то, ті ж зброю, визначені раніше для використання в захисті, порушення деградації, і заперечення атак. Зокрема, використання шифрування, підміни, впровадження шуму, перешкод і перевантаження, особливо корисні для підтримки збору інформації противника до мінімуму [88].

3.2. Організація, методи і засоби захисту національного інформаційного простору та інформаційного суверенітету

Щодо захисту інформаційного суверенітету, то він включає складні технології безпеки листування, телефонних дзвінків та приватного життя громадян. Яскравим прикладом порушення такого суверенітету є прослуховування та шпигунство спецслужбами однієї держави уряду іншої. Так, часто в ЗМІ виринають факти прослуховування Агентством національної безпеки США лідерів різних країн, в тому числі і України. Саме такі дії називають посяганням на інформаційний суверенітет. Боротися з таким явищем складно. Для протидії необхідно виробити ряд стратегій. Для цього необхідно розвивати та працювати одночасно над декількома

аспектами. По-перше, це законодавча база; по-друге, належне фінансування секретних програм для шифрування повідомлень та основних каналів зв'язку, які містять цінну інформацію; по-третє, розвивати технології, які будуть слугувати щитом для атак іноземних шпигунів; по-четверте, налагодити контроль над потоками інформації як вхідними, так і вихідними.

Саме для України останнім часом під час проведення «гібридної війни» з Російською Федерацією необхідним та вкрай важливим є дослідження і знаходження ефективних механізмів захисту національного інформаційного простору. Адже управляти народом і населенням, впливати на їх поведінку і свідомість, можна за допомогою засобів інформації, а тому кожна держава зацікавлена у забезпеченні національної інформаційної безпеки.

З цією метою в Україні створено Міністерство інформаційної політики, працює відповідний відділ СБУ. Згадане Міністерство покликане забезпечити здійснення функції, зокрема, тимчасового обмеження ретрансляції російських каналів (наразі обґрунтування цього обмеження слабке через нестачу моніторингу контенту та недооцінку ксенофобського аспекту в контенті російських ЗМІ).

Так, задля боротьби з російською пропагандою Міністерство інформаційної політики створило Інформаційні війська за аналогією із російськими, про що заявлено на офіційній сторінці Міністерства. Також у співпраці з волонтерами розроблено сайт і-*army.org*, а головним завданням даного проекту визначено мобілізацію користувачів соціальних мереж на донесення достовірної інформації та боротьби з російською пропагандою [88]. Основною функцією проекту визначено як об'єднання зусиль і протидія російським ботам, поширенню шейків(недостовірних новин та повідомлень), інформаційному і психологічному тиску російських ЗМІ.

МІП виступає головним органом у системі центральних органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, поширення суспільно важливої інформації в Україні та за її межами і

забезпечення функціонування державних інформаційних ресурсів, та проведення реформ ЗМІ щодо поширення суспільно важливої інформації. Відповідно до Положення Кабінету Міністрів України про МІП до кола основних завдань входять: 1) узагальнення практики застосування законодавства у сфері інформаційної політики; 2) розробка проектів законів та інших нормативно-правових актів; 3) вжиття заходів до захисту прав громадян на вільний збір, зберігання, використання і розповсюдження інформації, у тому числі на тимчасово окупованих територіях та у районі проведення антитерористичної операції; 4)координує діяльність органів виконавчої влади з питань інформаційної політики; 5) надає практичну допомогу прес-службам органів виконавчої влади; 6) розробляє плани захисту прав журналістів та споживачів інформаційної продукції; 7) здійснює дослідження впливу результатів діяльності ЗМІ на суспільну свідомість; 8) реалізує навчальні курси з інформаційної політики і розробляє навчально-методичне забезпечення для навчальних закладів; 9) розробляє документи, концепції щодо позиціонування України в світі; 10) розробляє стратегію захисту інформаційного простору України від зовнішнього інформаційного впливу; 11) повинно сприяти дотриманню в Україні свободи слова; 12) популяризує українську телепродукцію за кордоном; 13) здійснює моніторинг інформації у вітчизняних та іноземних засобах масової інформації [89].

У міжнародних відносинах суверенітет означає свободу, а саме, право бути «вільним від будь-якого зовнішнього контролю». Це право держави вільно реалізувати свою волю. Оскільки свобода в людському суспільстві завжди була «наближеною» замість «абсолютної», то це означає, що суверенітет повинен бути по крайній мірі близьким. Тільки тоді, коли країна ізолює себе повністю від навколишнього світу та інших країн, вона може насолоджуватися «абсолютною» свободою від зовнішнього втручання. Прикладом такої країни може бути Північна Корея. Та такі заходи безпеки,

як повна ізоляція відбирають у країни брати від інших позитивні надбання, такі, як природні ресурси, культуру, інноваційний обмін. Також держава не зможе розширити свій суверенітет від кордону та змусити інші держави дотримуватися своєї власної суверенної волі. В разі ізоляції вплив на власну територію – це все, що вона має. Саме тому, кожна держава сьогодні має «пожертвувати» трохи свого власного суверенітету в обмін на шанс співіснувати з іншими.

Звернення суспільної свідомості до проблем інформаційної безпеки пов'язано з новими особливостями життя в сучасному суспільстві. Як випливає із викладеного в попередніх розділах, виробництво стає більш інтелектомістким, інформаційно потужнішим. Все більша частина суспільства залучається до роботи з інформацією, і, в результаті, інформація стає найважливішим ресурсом суспільства. Поряд з поняттям «промисловість», «інфраструктура промисловості» все частіше в діловій мові ми зустрічаємо поняття «інформаційна індустрія», «інформаційна інфраструктуру». М. Кастельс зазначав, що прийдешня інформаційна епоха характеризується специфічною формою соціальної організації, в якій нові технології генерування, обробки і передачі інформації стали фундаментальним джерелом продуктивності і влади [82]. Складно не погодитися з тим, що сьогодні будь-яка соціальна практика, особливо пов'язана з виробництвом і управлінням, в широкому сенсі цього слова, актуалізує певний спектр інформації і обумовлена проблемою інформаційної безпеки [24, с. 60]

Також не можна не віддати належне фактичному мережевому характеру сучасних комунікацій, діяльністю соціальних мереж, мережевого принципу організації суспільства при вивченні соціальної природи інформаційної безпеки. Наведений аналіз впливу на формування суспільної думки, а також велика кількість емпіричних даних свідчать про популярність мережевого принципу сучасних соціальних комунікацій. Завдяки мережевому підходу

з’являється можливість організації різних соціальних інформаційних процесів, їх аналізу та диференціації на предмет небезпек, ризиків і загроз для різних соціальних суб'єктів.

Одна з головних функцій інформації, як соціального феномена, якій автор приділяє особливу увагу, полягає в наданні усвідомлюваного учасниками комунікаційних інтерактів соціально-культурного впливу на споживачів соціальної інформації, латентна - в неусвідомлюваному реципієнтами соціально-психологічному впливі, чиниться на них в ході даного виду комунікації. Виходячи з цього, загрози інформаційної безпеки суспільства, потенційно існуючі в процесі соціальної комунікації, в першу чергу призводять до негативних соціально-економічних наслідків для споживачів. Однак, в якості різновиду соціальної комунікації і виконуючи латентні функції, соціальна інформація зачіпає також інші види суспільних відносин (політичні, духовні і особистісні), що також може призводити до негативних змін в зазначених областях.

Таким чином, соціальна комунікація як феномен, що лежить в основі соціальної взаємодії, є ключовим механізмом функціонування культури і суспільства. Соціальна комунікація - це явище, що лежить в основі всіх соціальних зв'язків і відносин в суспільстві; це не тільки посередник між суб'єктами соціальної взаємодії, але сама форма існування таких суб'єктів; це не тільки спосіб освоєння смислового простору соціуму, а й засіб його конструювання. Більше того, на сьогоднішній день, соціальна комунікація здійснює неабиякий вплив в контексті забезпечення інформаційної безпеки держави. Дійсно, особливо важливим завданням суспільства є створення системи безпеки в сфері комунікацій та інформації.

На сьогодні, важко оспорити відхід від однозначної однолінійної, пропагандистської комунікації, де домінував жорсткий контроль над інформацією і одержувачем (адресатом). В інформаційному просторі сьогодення діють альтернативні види (багатовимірна, діалогічна,

консультативна і т.д.) комунікації. В результаті виникає потреба в пошуку ефективної моделі комунікації в цілому; такої, яка б відповідала сучасним принципам соціально-технічної організації життя суспільства і держави.

Розвиток інформаційних технологій, глобальна комп'ютеризація всіх сфер життєдіяльності, актуалізація проблем соціального виробництва, «якості життя» всіх верств громадянського суспільства висувають на перший план залучення в процес комунікації не тільки привілейованих суб'єктів (держава, суспільно-політичні організації), а й диктує необхідність враховувати формування громадянського суспільства у всій складності його структури, соціальної диференціації (при цьому, в Західні держави вже зіштовхнулись з таким феноменом як «громадянське суспільство»). На зміну імперативу класичної політичної комунікації приходять механізми підтримуючої комунікації (діалогічного, емпатичних і т.д.) як умова для вільного життєзабезпечення і реалізації життєвих потенцій кожної людини, як запорука громадського порядку в цілому. Метою соціально-політичної комунікації є гарантоване отримання політичної стабільності в регіоні, країні, світі. Основна функція - регулювання суспільних відносин у всіх сферах суспільного життя. Стабільність громадянського суспільства стає основною турботою і держави, і всіх суспільно-політичних інститутів країни. У новому соціальному просторі, що формується буквально на наших очах, зазнають значних змін і моделі комунікації, їх зміст, цілі, структура та функції. Ці аспекти вимагають їх безпосереднього врахування при розбудові інформаційної безпеки держави.

Виходячи з загальних рис, властивих кожній державі в контексті розбудови державності, а також враховуючи різний економічний розвиток та культурний, соціальний, релігійний та інші суспільні «фони», як складової будь-якої держави, а також враховуючи велику кількість різних моделей соціальних комунікацій, ми пропонуємо «апгрейд» загальної концептуальної моделі, яка б описала реальні можливі дії, які можуть бути різних чином

ускладнені, та врахувала позицію автора з точки зору соціокомунікаційного впливу на інформаційну безпеку держави.

На нашу думку, модель інформаційної безпеки в соціокомуінкаційному вимірі має включати наступні елементи:

• суб'єкти / учасники комунікативного процесу:

- Суб'єкти громадянського суспільства (політичні і громадські партії, руху і т.д.);

- Засоби масової інформації та комунікації як юридичні особи, щодо інформаційної політики - редакції ЗМІ;

- Професійні медіа-групи - групи (спільноти), об'єднані спільною професійною діяльністю / інтересами (в тому числі виділяються в рамках більш великих структур, наприклад - організацій) і проводять в інформаційному просторі самостійну інформаційну діяльність;

- Медіа-персони - особи (перш за все, пересічні громадяни), які використовують інформаційний простір для актуалізації в ньому своїх приватних інтересів на рівні масової комунікації (не в останню чергу вищезгадана мережева комунікація);

- Держава

При цьому, компетентність суб'єктів не обмежена принциповим чином: державні органи діють відповідно до визначених приписів, а діяльність інших суб'єктів в Інтернеті регулюються ad hoc приписами, оскільки а пріорі на них поширюються принцип свободи слова. В цьому ключі представляється доцільним для державних інститутів проводити оперативний моніторинг сайтів, покликаних підірвати соціальну, політичну чи навіть державну стабільність, прогнозувати можливі соціально-політичні наслідки від роботи таких сайтів, а в деяких випадках - і створювати альтернативні сайти на противаг «ворожим».

- Необхідно відзначити, що вищезазначені суб’єкти в контексті інформаційної безпеки можуть бути об’єктами впливу, особливо це стосується фізичних та юридичних осіб.

• Контекст комунікації варіюється; в рамках дослідження він не набуває принципового значення, оскільки основний контекст – інформаційна безпека держави; динаміка контекстів комунікації в дії (фізичний, соціальний, психологічний і культурний).

• Повідомлення, яке передається від одного суб’єкта до іншого (комуніканти), конвертується відповідно до його і передається через відповідні канали (вербальні, невербальні, паравербальні); значення, представлені символами, знову перетворюються комунікантами в значення в процесі декодування, який повністю визначається життєвим досвідом коммуникантов, як і в процесі кодування;

• Шуми (у випадку соціокомунікаційного виміру в контексті національної безпеки держави, в якості шуму слід розглядати як вплив – на сприйняття, розуміння та відповідні посили повідомлень, що генеруються внутрішніми та зовнішніми суб’єктами, які, як правило, є загрозою для безпеки держави), що виникають в будь-якій точці процесу і мають вплив на можливість створення переданого значення;

• При цьому, в процесі комунікації, приєднуються і «соціокультурні фільтри» як механізм впливу на процес комунікації, в яких, за нашим задумом, дуже добре орієнтується третій суб’єкт при впливі на комуніканта на етапі передачі повідомлень (створення шуму).

• Значення комунікації в цьому ключі буде подвійне, адже первинне завдання, поставлене комунікантом, видозмінюється на етапі впливу шумів і тому, адресат може діяти по іншому;

• Зворотній зв'язок, при якому мовець враховує сигнали і шукає нові, більш ефективні тактики мовної поведінки для успішної реалізації комунікативного задуму, він вже діє відповідно до «запрограмованих

установок» і генерує в контексті мережевого спілкування «викривлені» повідомлення (меседжі), які часто можуть спричинити лавиноподібно проблеми для національної безпеки держави

Ця модель набуває особливої актуальності для соціально-політичної комунікації, де має значення і освіченість комунікантів, і включеність в загальносоціальний контекст, і свого роду «прогресивність» в контексті володіння і користування сучасними комунікаційними технологіями (соціальні мережі в першу чергу). Так, суспільство як система характеризується непорушним протиріччям між інтересами особистості і соціальним порядком. Інтереси суб'єктів виражаються через різні суспільно-політичні структури: політичні партії, профспілки, союзи підприємців, лобістські структури, громадські організації. У механізмах, за допомогою яких здійснюється зв'язок між громадянами і державою, суттєва роль належить групам інтересів і групам тиску. Групи інтересів - це добровільні об'єднання громадян, які не є політичними партіями. Вони створюються для вираження і представництва інтересів людей у взаєминах з іншими групами і політичними інститутами.

А. Бентлі, автор концепції груп інтересів, стверджував, що свої інтереси індивіди здійснюють за допомогою груп, в які вони об'єднані на основі спільності інтересів. Індивідуальні переконання, окремі ідеї і особистісні характеристики поведінки мають значення лише в контексті діяльності групи і враховуються в тій мірі, в якій вони допомагають при розробці моделей групової поведінки. Відмінності в політичних режимах А. Бентлі представляв як відмінності в типах групової діяльності або в техніці групового тиску. Наростання різнорідності соціальних інтересів призводять до появи різноманіття зацікавлених груп, автономних по відношенню один до одного (наприклад, груп від бізнесу, профспілок, фермерів, інтелектуалів). Політичні рішення в цих умовах перестають бути прерогативою офіційних інститутів влади, а стають результатом компромісу суперечливих груп інтересів. Групи

інтересів мають широкі можливості впливу на владу, а відповідно, на життя суспільства в цілому. У такій якості вони виступають як групи тиску. Можливими способами впливу (тиску) можуть виступати їх економічні та фінансові ресурси, інформація та досвід політичної участі їх членів, організаційні структури та ін. Залежно від значення для політичної системи відповідних владних ресурсів груп інтересів останні мають певну вагу при прийнятті управлінських рішень. На противагу цьому спроби впливу на владу маргінальних, нетрадиційних груп інтересів, які ігнорують діючі в суспільстві норми і цінності, можуть мати руйнівну дію для існуючого соціального порядку. Ці спроби впливу зазвичай заперечуються соціальною системою.

США беруть найактивнішу участь в процесі формування міжнародної політико-правової бази в області інформаційної безпеки і фактично є єдиною країною, представленою у всіх регіональних організаціях, до порядку денного яких включено питання кіберполітики. Таке широке міжнародне представництво дає США можливість активно просувати власні ініціативи, а також координувати міжнародні зусилля в цій галузі. При цьому існує ряд причин, що ускладнюють роботу міжнародного співтовариства щодо формування глобального режиму інформаційної безпеки.

У доповіді Комісії з кібербезпеки для 44-го президента в 2008 р. зазначається, що «нездатність Америки захистити кіберпростір є однією з найбільш гарячих проблем національної безпеки, що стоять перед Адміністрацією».

Рада безпеки РФ запропонувала розробити нову доктрину інформаційної безпеки РФ, так як діючий документ не враховує всіх сьогоднішніх реалій, пов'язаних з бурхливим розвитком інформаційних технологій. Загрози, з якими може зіткнутися суспільство, - це інформаційна війна, викрадення персональних даних, кібершахрайство. Нова доктрина має бути прийнята вже

цього року. Так, в результаті ознайомлення в проектом документу, можна говорити про такі ключові його положення.

У вступі уточнюється, що доктрина «є документом стратегічного планування у сфері забезпечення національної безпеки РФ» і служить основою «для вироблення заходів з розвитку системи інформаційної безпеки РФ», «розробки і виконання державних програм» в цій сфері, а також «організації співпраці РФ з іншими державами і міжнародними інститутами».

Далі описуються переваги ІКТ. Відзначається, що вони «стали невід'ємною частиною всіх сфер діяльності особистості, суспільства і держави», що їх «ефективне використання є фактором прискорення економічного розвитку і сприяє формуванню суспільства знання», а «інформаційна сфера відіграє важливу роль в забезпеченні політичної стабільності в країні, оборони і безпеки держави».

У Росії, як випливає з проекту документа, є ряд національних інтересів в інформаційній сфері, включаючи «дотримання конституційних прав і свобод людини і громадянина в області отримання та використання інформації, включаючи недоторканність приватного життя», «розвиток галузі інформаційних технологій в РФ», «забезпечення сталого розвитку та безперебійного функціонування інформаційної інфраструктури РФ в мирний час, в період безпосередньої загрози агресії і у воєнний час», «доведення до російської і міжнародної громадськості достовірної інформації про державну політику РФ» і «сприяння поширенню духовних і культурних цінностей народів Росії по всьому миру».

По-перше, попереджають вони, закордонні країни нарощують потенціал в сфері ІКТ, в тому числі для впливу на критичну інформаційну інфраструктуру РФ (електромережі, системи управління транспортом і т. д.) І технічної розвідки щодо російських держорганів, наукових організацій і підприємств оборонно-промислового комплексу.

По-друге, як випливає з проекту доктрини, спецслужби і «підконтрольні громадські організації» окремих держав активно використовують ІКТ «як інструмент для підриву суверенітету і територіальної цілісності» інших країн, «дестабілізації внутрішньополітичної та соціальної ситуації». При в цьому в якості загрози розглядається і «тенденція збільшення обсягу матеріалів в зарубіжних ЗМІ, що містять необ'єктивну і упереджену інформацію про зовнішню і внутрішню політику РФ», а також «нарощування інформаційного впливу на населення країни, в першу чергу на молодь, з метою розмивання культурних і духовних цінностей, підриву моральних підвалин, історичних основ і патріотичних традицій».

По-третє, в документі вказується на зростання масштабів комп'ютерної злочинності, перш за все в кредитно-фінансовій сфері, і збільшення числа інцидентів, пов'язаних з порушенням законних прав громадян на недоторканність приватного життя.

По-четверте, констатується «відставання РФ від провідних зарубіжних держав у створенні конкурентоспроможних ІКТ і продукції на їх основі» (в тому числі суперкомп’ютерів і електронної компонентної бази), що зумовлює залежність країни від експортної політики інших держав.

По-п’яте, загрозою визнано «прагнення окремих держав використовувати для досягнення економічного і геополітичного переваги технологічне домінування в глобальному інформаційному просторі». «Окремі держави» не перераховуються, але мова йде, по всій видимості, про США.

Примітно, що в розділі, присвяченому інформаційної безпеки в області оборони, також сказано про необхідність «протидії діяльності з інформаційного впливу на населення і в першу чергу на молодих громадян країни, що має на меті підрив історичних, духовних і патріотичних традицій в області захисту вітчизни».

Цій темі автори доктрини приділяють увагу і в розділі, присвяченому державної і громадської безпеки. Крім боротьби з використанням ІКТ з

метою пропаганди ідеології тероризму, екстремізму та ксенофобії, влади РФ вважають за необхідне протидіяти залученню Інтернету для поширення ідей національної винятковості (ймовірно, відсилаючи до відомого заявою президента Барака Обами про «винятковості» США), підриву суспільно-політичної стабільності, насильницької зміни конституційного ладу РФ.

У цьому ж розділі є абзац, де йдеться про захист критичної інформаційної інфраструктури РФ від комп'ютерних атак. Але в порівнянні з захистом населення від «згубного впливу ззовні», цієї найважливішої темі в проекті документа приділено напрочуд мало уваги.

Однак, як випливає з тексту доктрини, всьому цьому може перешкодити безліч загроз: інформаційний простір все частіше використовується «для вирішення військово-політичних завдань, а також в терористичних та інших протиправних цілях». Укладачі доктрини виділяють п'ять блоків загроз для нацбезпеки країни в інформаційній сфері.

Стратегія інформаційної безпеки Японії так само була прийнята достатньо давно - в травні 2010 р. Її так само можна проаналізувати в наступних розрізах:

- посилення політики з урахуванням можливих спалахів кібер-атак і створення організацій для відповідного реагування;

- проведення політики, адаптованої до змін у середовищі інформаційної безпеки;

- здійснення активних, а не пасивних заходів із забезпечення інформаційної безпеки.

Основні напрямки дій, охоплені стратегією, включають:

- долати IT-ризики для реалізації загальної безпеки і суспільної безпеки;

- здійснення політики, яка посилює національну безпеку і кризову управління знаннями в кіберпросторі, і цілісність з політикою в сфері ІКТ як основи соціально-економічної діяльності;

- створення політики тріади, яка всебічно охоплює національну безпеку, кризове управління і захист нації/користувача. Політика інформаційної безпеки, що фокусується на користувачах, є особливо важливою;

- створення політики інформаційної безпеки, яка робить внесок у стратегію економічного зростання;

- формування міжнародних альянсів.

Більше того, у Японії крадіжка особистої, ділової і організаційної інформації та активів відбувається все частіше. Існують також зростаючі загрози, спрямовані проти національної безпеки, безпеки державних органів та бізнесу, які забезпечують критично важливі інфраструктури, необхідної для повсякденного життя людей і економічної діяльності. На ці структури часто відбувалися кібер-атаки.

У цих умовах Японія прийняла закон про основні засади з кібербезпеки в листопаді 2014 р. Цей закон передбачає поняття кібербезпека і визначає ролі та обов'язки уряду, місцевих органів влади та інших відповідних зацікавлених сторін; він також позначає Агентство кібербезпеки як контрольний орган національної кібербезпеки. Цей документ розглядає захист національної інформаційної безпеки на найближчі 4 роки з подальшими перспективами та планами розвитку країни.

Кіберпростір це штучно створений простір для вільного обміну інформацією, необмежений національними кордонами; це нематеріальна межа нескінченних значень, породжена інтелектуальною творчістю та інноваціями, це натхненний ідеями по всьому світу обмін. Інвестиції приватного сектора під керівництвом і накопичення знань зіграли ключову роль в швидкому розширенні кіберпросторі; і, сьогодні, кіберпростір є найважливішою основою соціально-економічної діяльності в Японії, так як він привернув велику кількість користувачів через його недискримінаційний характер.

У той час як кіберпростір приніс значні вигоди для нашого життя, загрози національній інформаційній безпеці теж збільшились. Такі атаки можуть бути як зі сторони приватних осіб, так і зі сторони держав.

Основними завданнями Японії на цьому напрямку є: забезпечення вільного, справедливого та безпечного кіберпростору; сприяти поліпшенню соціально-економічної життєздатності і сталого розвиток, побудова суспільства, де люди можуть жити спокійним і безпечним життя, а також забезпечення миру і стабільності міжнародного співтовариства і національної безпеки.

В програмі уряд Японії відзначив 5 основних принципів захисту національної інформаційної безпеки.

1. Забезпечення вільного потоку інформації

При розгляді правил в кіберпросторі, вільний потік інформації повинен бути повністю поважитись, і особливу увагу слід приділяти захисту індивідуальної недоторканості приватного життя. У цьому сенсі слід підтримувати належний баланс між необхідними правилами і захистом приватного життя.

2. Верховенство закону

У взаємопов'язаному і конвергентному інформаційному суспільстві верховенство закону має ретельно застосовується до кіберпростіру таким же чином, як він застосовується в фізичному просторі. В Японії, кіберпростір підпорядковується законам і інші правилам і нормам не тільки на державному, а й на міжнародному рівні. Японія буде продовжувати приймати активну участь в розробці і реалізації міжнародних норм і правил, а також діяти на стаціонарному введення таких правил і норм в кожній країні ґрунтуючись на своїх внутрішніх ситуаціях.

3. Відкритість

Уряд Японії підтримує думку, що кіберпростір не повинно бути виключно у владі певної групи акторів, а має бути відкритим для всіх людей,

які хочуть використовувати його, оскільки кіберпростір з'єднує ідеї і знання, і приносить нові цінності. Та все ж інформація має бути такою, що не шкодить державі та не принижує інших.

4.Автономія

Інтернет дає можливість розвиватись не лише державі, а й приватним особам, які у власних цілях використовують кіберпростір. Тому проблеми захисту інформаційного простору повинна вирішувати не лише держава, а й приватні особи.

5. Співпраця

Кіберпростір є багатовимірним, що складається з різних зацікавлених сторін та діяльності в різних шарах. З цієї точки зору, необхідно щоб всі зацікавлені в національній інформаційній безпеці сторони обєднували зусилля.

На цих п’яти принципах ґрунтуватиметься політика Японії та співпраця з приватними особами, а також іноземними державами. Законотворчість в даному випадку буде направлена на модернізацію існуючої та створеної нової системи захисту.

Робота держави та державних установ у даному полі буде направлена на:

- Запобігання інцидентів кібератак;
- Запобігання ушкодження і поширення ушкоджень;
- Пом’якшенння завданих збитків;
- Досягнення стійких організаційних можливостей реагування;
- Адаптація до технологічного розвитку і змін;
- Всебічне підвищення ефективності заходів щодо розширення області застосування моніторингу.

Що ж до Австралії, якось колишній прем`єр-міністр Австралії сказав: «... Витонченість нашого сучасного суспільства є джерелом уразливості самим по собі .... ми в значній мірі залежимо від комп'ютерних та інформаційних технологій для підвищення продуктивності галузей, таких як авіація;

електропостачання та водопостачання; банківська справа і фінанси; телекомунікаційні мережі. Ця залежність від інформаційних технологій робить нас потенційно уразливими для кібер-атак, які можуть порушити інформацію, яка все більше і більше проникає в нашу економіку і систему управління».

В Австралії уряд розгорнув широку та масштабну кампанію щодо попередження небезпеки для національної інформаційної безпеки в 2008 році. Сьогодні радіо, телебачення та друковані ЗМІ активно публікують різну соціальну рекламу. Зокрема в газетах Австралії можна натрапити на номер телефону гарячої лінії Агентства з національної безпеки разом з наступним повідомленням: «Кожна інформація, яку ми отримуємо від представників громадськості сьогодні може виявитися неоціненною для безпеки Австралії завтра. Всі деталі мають велике значення. Тож якщо ви бачите або чуєте щось, що вас бентежить, будь ласка, зателефонуйте до гарячу лінію» З такою ж інформацією транслюють повідомлення на радіо.

Відповідно до затвердженої урядом стратегії кібер-безпеки та національній інформаційній безпеки Австралії, його діяльність ґрунтується на наступних принципах.

Національне лідерство. Масштаби і складність кібербезпеки та національної інформаційної безпеки вимагає сильного національного керівництва.

Загальні обов'язки. Всі користувачі, які користуватися перевагами інформаційних технологій та ЗМІ, повинні вживати необхідних заходів для забезпечення своїх власних даних, проявляти обережність в спілкуванні і зберігати конфіденційну інформацію, і зобов'язані поважати інформацію та конфіденційність інших користувачів.

Партнерство. У світлі цих загальних обов'язків, партнерський підхід до кібер-безпеки та безпеки інформації австралійського уряду, приватного сектора і австралійського суспільства має важливе значення.

Активна міжнародна участь. З огляду на транснаціональний характер Інтернету, в якому ефективна кібербезпека вимагає скоординованих глобальних дій, Австралія повинна взяти активний, багаторівневий підхід до міжнародної участі у забезпеченні власної національної інформаційної безпеки.

Управління ризиками. У глобалізованому світі, де всі інтернет-системи пов'язані і потенційно вразливі, де кібер- та інфо- атаку важко виявити, немає такого поняття, як абсолютна безпека. Тому Австралія повинна застосовувати підхід на основі ризику для оцінки, визначення пріоритетів і виділення ресурсів діяльності щодо забезпечення безпеки.

Захист австралійських цінностей. Австралія повинна проводити політику безпеки, яка підвищує індивідуальну та колективну безпеку, зберігаючи при цьому право австралійців на приватне життя та інших основоположні цінності та свободи. Підтримка цього балансу є постійним завданням для всіх сучасних демократій, які прагнуть вирішити складні проблеми кібер-безпеки в майбутньому.

Загалом типовим для усіх країн світу є вироблення механізмів забезпечення інформаційної безпеки держави у соціально-комунікаційному плані такими засобами: забезпеченням балансу інтересів особи, суспільства та держави; системне вироблення концепції держави у сфері національної безпеки і соціально-комунаційної сфери загалом, комплексний підхід – налагодження співпраці не тільки між усіма державними органами, що забезпечують безпеку у державі – наприклад Міністерством закордонних справ, Міністерством інформаційної політики та Міністерством оборони, активна співпраця із науковими інституціями та науково-дослідними інститутами, але і інтеграція з міжнародними системами безпеки, входження в єдині уніфіковані правила забезпечення інформаційної безпеки. Зокрема, забезпечення інформаційної безпеки держави залежить також від ефективності публічної демократії, налагодження зв’язків між державами,

покращення співпраці шляхом проведення міжнародних конференції, комунікації.

Створення і застосування єдиних уніфікованих стандартів усіма суб'єктами сприятиме забезпеченню безпеки інформаційних систем. Так, в «ЄС діє Організація європейського співробітництва з питань акредитації (European cooperation for accreditation), що забезпечує сертифікацію бізнес-процесів та систем управління інформаційною безпекою, Європейська ініціатива з питань стандартизації електронних підписів (European Electronic Signatures Standardisation Initiative), спрямована на розробку єдиних рішень на підтримку директиви ЄС про електронні підписи, а також ініціативи впровадження інфраструктури з відкритими ключами» [90].

Головна проблема - існування величезної кількості конкуруючих стандартів і специфікацій, що призводить до фрагментації ринку та важкості знайти єдиний уніфікований підхід. Основним завданням виступає гармонізація та уніфікація усіх стандартів.

Усі держави світу і Україна не є винятком має налагоджувати і покращувати міжнародне співробітництво в інформаційній сфері. Так, у рамках ENISA, підтримуються проекти співробітництва країн-членів ЄС у сфері інформаційної політики.

Так, «ENISA надала підтримку проектам співпраці між Угорщиною та Болгарією щодо створення Болгарської урядової комп'ютерної групи швидкого реагування (CERT), а також співробітництва між CERT-FI (Фінляндія) та CSIR/MERAKA (Південна Африка) щодо обміну досвідом та створення Південно-африканської групи реагування на комп'ютерні інциденти (Computer Security Incident Response Team)».

ENISA також сприяла розвитку партнерства між приватними і державними структурами щодо обміну інформацією про кіберзлочини між фінансовим сектором і державними органами через Центри фінансової інформації та аналізу (FI-ISAC).

«Фінляндія займає лідируючі позиції серед країн ЄС за показниками розвитку інформаційного суспільства». В рейтингу країн ЄС Фінляндія займає перше місце за рівнем цифрової грамотності (понад 50% населення), Основними державними установами, відповідальними за розробку та реалізацію політики інформаційної безпеки, є Міністерство транспорту та комунікацій та Омбудсмен з питань захисту даних (Data Protection Ombudsman) тощо.

Повноваженнями Міністерства транспорту та комунікацій є розробка законодавства щодо комунікаційних мереж, безпеки даних, забезпечення доступу до комунікаційних послуг, а також вироблення і реалізація національної політики в сфері інформаційної безпеки. Інформаційна безпека визначається як комплекс адміністративних та технічних заходів щодо забезпечення конфіденційності та цілісності інформації, а також зручності користування інформаційною системою.

У грудні 2008 року урядом Фінляндії прийнято Національну стратегію інформаційної безпеки.

У Стратегії визначено п’ять пріоритетних цілей державної політики в сфері інформаційної безпеки, а саме:

1. розвиток співпраці з питань інформаційної безпеки на міжнародному і національному рівнях;

2. підтримання національної конкурентоспроможності та створення сприятливих умов для національних операторів інформаційно-комунікаційних технологій;

3. поліпшення системи контролю над можливими загрозами інформаційній безпеці держави;

4. забезпечення захисту основоположних прав і свобод громадян та інтелектуального потенціалу держави;

5. підвищення громадської обізнаності в сфері інформаційної безпеки.

Діяльність з розвитку національного і міжнародного співробітництва в сфері інформаційної безпеки передбачає реалізацію таких заходів: створення Консультативної Ради з питань інформаційної безпеки, уповноваженої контролювати виконання стратегії; участь у розробці законодавства та стандартів в сфері інформаційної безпеки в рамках ЄС та міжнародних організацій; започаткування дослідницького проекту щодо важливості довіри і інформаційної безпеки в сучасному суспільстві; надання підтримки державних суб'єктам у зміцненні інформаційної безпеки.

За другим пріоритетним напрямом передбачаються такі заходи, як забезпечення доступності інформації про інформаційну безпеку для компаній та інших організацій; сприяння розвитку інновацій в сфері інформаційної безпеки, формуванню експертних мереж між організаціями та розвитку співробітництва між державним і приватним секторами; надання підтримки компаніям та дослідницьким інститутам у виробництві нових засобів/продуктів інформаційної безпеки; створення умов для підвищення сумісності інформаційних систем/мереж в державному та приватному секторах; проведення регулярної оцінки впливу законодавства та міжнародних договорів в сфері інформаційної безпеки на комунікаційні послуги, банківські онлайн послуги, послуги електронної ідентифікації, е-комерцію та електронні транзакції в діловій сфері.

Для вдосконалення системи управління ризиками в сфері інформаційної безпеки передбачається реалізація таких заходів: створення системи моніторингу та здійснення регулярної оцінки ризиків інформаційній безпеці; розробка методів аналізу вразливостей в сфері інформаційної безпеки; створення робочої групи з питань інформаційної безпеки під керівництвом Консультативної Ради з питань інформаційної безпеки.

Діяльність щодо захисту фундаментальних прав та національного інформаційного капіталу включає забезпечення свободи висловлення, конфіденційності комунікацій, захисту недоторканості приватного життя та

інших громадянських прав, які мають бути враховані у законодавстві та стандартах, що стосуються інформаційного суспільства та інформаційної безпеки тощо.

Для підвищення обізнаності та компетентності в сфері інформаційної безпеки передбачено такі заходи, як дослідження сучасного рівня обізнаності та компетентності в сфері інформаційної безпеки, визначення потрібного рівня компетентності та започаткування необхідних проектів для підвищення загального рівня обізнаності громадськості з питань інформаційної безпеки; поширення фактичної інформації та впровадження курсів з інформаційної безпеки на всіх рівнях шкільного навчання; сприяння розробці та використанню сертифікатів якості в сфері інформаційної безпеки тощо.

Структурним підрозділом Міністерства транспорту та комунікацій є Управління Фінляндії з регулювання комунікацій (Finnish Communications Regulatory Authority – FICORA), яке уповноважене здійснювати контроль та державне регулювання сфери інформаційно-комунікаційних технологій. Запорожець О.Ю.

Основне призначення FICORA полягає у забезпеченні ефективних та безпечних комунікаційних з'єднань та послуг, а також у сприянні розвитку інформаційного суспільства.

До повноважень FICORA відноситься контроль функціональності електронних комунікаційних мереж, інформування про можливі загрози інформаційній безпеці, підвищення обізнаності громадян з питань інформаційної безпеки, планування і управління використанням радіочастот, мережевими адресами, а також контроль змісту програм і реклами на телебаченні та радіо.

У Стратегії FICORA на 2009-2015 роки визначено такі пріоритетні напрями діяльності установ:

- забезпечення високоякісних та прийнятних за ціною комунікаційних послуг для громадян та компаній Фінляндії;

- забезпечення швидких і надійних телекомунікаційних послуг;

- захист прав громадян як користувачів комунікаційних послуг (зокрема, поширення інформації про ціни, якість та інші характеристики комунікаційних послуг; розробка єдиної системи вимог до компаній, що надають телекомунікаційні послуги тощо);

- забезпечення високоякісних медіа послуг за прийнятними цінами для всіх громадян, відстеження шкідливого для дітей контенту телепрограм, сприяння підвищенню медіаграмотності громадян;

- підвищення обізнаності громадян з питань інформаційної безпеки і захисту приватного життя та забезпечення конфіденційності комунікацій;

- забезпечення функціональності ринку комунікацій (аналіз конкурентного середовища, моніторинг цін на телекомунікаційні послуги тощо);

- забезпечення ефективного розподілення радіочастотних діапазонів;

- зміцнення інформаційної безпеки на корпоративному рівні;

- встановлення стандартів інформаційної безпеки для національних комунікаційних систем і продуктів;

- сприяння розвитку співробітництва між компаніями, які надають телекомунікаційні послуги;

- поліпшення технічної якості та надійності комунікаційних мереж і послуг.

В структурі FICORA функціонує CERT-FI (Computer Emergency Response Team of Finland) – фінська комп'ютерна група швидкого реагування, завданням якої є підтримання безпеки в інформаційному суспільстві шляхом попередження, виявлення та реагування на інциденти в сфері інформаційної безпеки (information security incident), а також поширення інформації про загрози інформаційній безпеці.

CERT-FI здійснює моніторинг інцидентів на національному рівні і веде статистику. Підрозділ отримує повідомлення про безпекові інциденти від

операторів телекомунікаційних послуг, а також від державних та приватних організацій. До компетенції CERT-FI також відноситься: підтримання обізнаності громадськості про загрози інформаційній безпеці; вироблення рекомендацій для зміцнення інформаційної безпеки; поширення інформації про способи попередження інцидентів, пов'язаних з інформаційною безпекою; надання допомоги у вирішенні проблем в сфері інформаційної безпеки; співробітництво з постачальниками обладнання та програмного забезпечення, з правоохоронних органами; проведення моніторингу і аналізу загроз інформаційній безпеці на міжнародному рівні тощо.

Омбудсмен з питань захисту даних (Data Protection Ombudsman) - незалежний орган, уповноважений забезпечувати захист права громадян на недоторканість приватного життя шляхом здійснення контролю за обробкою персональних даних та надання консультацій з цих питань. Омбудсмен спільно з FICORA видає спеціалізований журнал «Tietosuoja», присвячений проблемі захисту даних. Журнал містить інформацію про норми і практику в сфері захисту даних, про безпеку даних в електронних системах комунікації, а також вимоги ЄС щодо рівня захисту даних в країнах-членах

Серед неурядових організацій, які займаються питаннями інформаційної безпеки, провідна роль належить Фінській федерації комунікацій та телеінформатики (Finnish Federation for Communications and Teleinformatics – FiCom) та Фінській асоціації з питань інформаційної безпеки (Finnish Information Security Association).

Фінська федерація комунікацій та телеінформатики об'єднує компанії, що працюють в сфері інформаційно-комунікаційних технологій. Основна мета діяльності федерації – розвиток бізнес-можливостей своїх членів та підвищення їхньої конкуретоспроможності. Діяльність FiCom включає планування і координацію заходів щодо розвитку інформаційно-комунікаційних технологій, здійснення моніторингу ситуації в ІКТ-секторі, здійснення впливу в сфері регулювання ринку інформаційно-комунікаційних

технологій тощо. Федерація підтримує тісні контакти з політичними діячами, державними службовцями, представниками ЗМІ та іншими організаціями.

Фінська асоціація з питань інформаційної безпеки є найбільшою неприбутковою асоціацією Фінляндії в сфері інформаційної безпеки, яка функціонує з 1997 року й об'єднує понад 90 членів. Метою діяльності асоціації є розвиток професіоналізму й обізнаності в сфері інформаційної безпеки. Діяльність асоціації включає організацію дискусій, конференцій, участь у різних програмах з інформаційної безпеки.

В країні реалізується низка програм в сфері інформаційної безпеки, що фінансуються урядом Фінляндії. Такими програмами є Фінський проект з Інтернет-обізнаності та безпеки (The Finnish Internet Awareness and Safety project), Проект Інтернет довіри (TrustInet Project) та Інтернет-автобус (Internet Bus) [7].

Фінський проект з Інтернет-обізнаності та безпеки, розрахований на період 2008-2010 роки, є спільним проектом трьох організацій: «Save the Children Finland», Ліга захисту дітей імені Маннергейма (The Mannerheim League for Child Welfare) та FICORA. Метою проекту є просування безпечного користування мережею Інтернет та боротьба з незаконним контентом. В рамках проекту реалізуються такі заходи, як організація Дня безпечного Інтернету, створення навчальних програм з питань безпеки Інтернет для провайдерів веб-контенту, встановлення «телефону довіри» для користувачів Інтернет для повідомлення про незаконний контент та інші проблеми.

Суть проекту TrustInet полягає у дослідженні проблеми довіри у відносинах між провайдерами послуг та споживачами в мережі Інтернет. Проект фінансується Державним агентством фінансування технологій та іновацій (Finnish Funding Agency for Technology and Innovation - Tekes), яке виділило 1,8 мільойнів євро на створення експертної групи «Надійний Інтернет» (Trustworthy Internet) в Гельсинському Інституті інформаційних

технологій, Лабораторії телекомунікацій та мультимедіа в Гельсинському технологічному університеті та Комп'ютерного департаменту в Гельсинському національному університеті.

З червня 2001 року реалізується проект «Інтернет-автобус», що має за мету навчити людей працювати з комп'ютерами та користуватися мережею Інтернет. У фінському місті Тампере їздить яскраво розмальований автобус «Netti-Nysse», обладнаний комп'ютерами, в якому проводяться навчальні курси з комп'ютерної грамотності. Навчальні групи складаються з 7-10 осіб. Тренінг триває 2 години. Тренінги проводять досвідчені спеціалісти по роботі зі споживачами.

Вважаємо за доцільне першочергово розглянути практичний досвід Естонії у реалізації стратегії інформаційної безпеки, що дійсно є взірцем для наслідування та очолює «рейтинг» країн по інформаційній безпеці. В даній країні провідне місце у забезпеченні інформаційної безпеки належить Міністерству економіки і комунікацій, що реалізує безпосередньо державну політику інформаційної безпеки. У складі Міністерства дану функцію в першу чергу виконує Департамент державної інформаційної системи і Естонський центр інформатики.

Департамент державної інформаційної системи Естонії уповноважений покликаний створити правове поле для реалізації інформаційної безпеки і здійснювати контролб за політичною діяльністю, створювати плани щодо загальнонаціональних адміністративних інформаційних систем(бюджети, застосування проектів інформаційних технологій, проведення аудиту, створення державних стандартів, налагодження міжнародного співробітництва щодо національних інформаційних систем. Даний департамент фактично займає ключову позицію у забезпеченні інформаційної безпеки Естонії і виконує функцію фактично законодавчого органу, що надає рекомендації парламенту у сфері інформаційних систем.

Натомість Естонський центр інформатики реалізує політику у сфері інформаційних систем, яку пропонує Департамент державної інформаційної системи і керує створенням та управлінням державною інформаційною системою.

Предмет відання Естонського центру інформатики охоплює:

- створення IT-проектів для усіх державних установ
- відстеження новітніх інформаційних технологій та ноу-хау
- покращення існуючих комп'ютерних мереж
- проведення державних закупівель інформаційних технологій
- виготовлення і створення державних реєстрів.

Як у всіх інших державах, що досліджуються, в Естонії також створено Міністерством економіки та комунікацій стратегію інформаційної безпеки та створено державну політику щодо інформаційної безпеки. Основне завдання інформаційної безпеки Естонії - побудова інформаційного суспільства, що відкрите до міжнародного діалогу з інформаційної безпеки, мінімізує ризики, що можуть виникнути у сфері інформаційної безпеки; політика спрямована на захист основоположних прав і свобод людини, донесення інформації до громадян шляхом її презентації, проведення тренінгів, сприяння покращенню економіки держави.

Стратегію інформаційної безпеки Естонії можна розподілити за наступними сферами:

1. Створення електронної безпеки держави за допомогою координації та співпраці усіх органів державної влади. Основну роль у забезпеченні даної функції відіграє Міністерство економіки та комунікацій, що здійснює аналіз загроз середовищу інформаційно-комунікаційних технологій Естонії, керівництво спеціальною технологічною групою миттєвого реакції на загрози в інформаційній сфері, що діє в Естонії, співпрацює з Європейською

агенцією щодо мережевої та інформаційної безпеки, здійснює реалізацію усіх міждержавних ініціатив.

2. Міністерство внутрішніх справ і Міністерство оборони забезпечують контроль за кризовим управлінням і кіберзлочинністю, що передбачають створення стратегії державного управління в кризових умовах, налагодження співпраці усіх органів державної влади, активізацію діяльності держави у міжнародних заходах щодо кіберзлочинності.

3. Міністерство освіти та науки, Міністерство оборони, Міністерство економіки і комунікаці, а також Державна канцелярія забезпечують збільшення рівня знань та поінформованості з питань загроз інформаційній безпеці держави, захисту від кібератак, шляхом проведення семінарів, презентацій, створення сайтів, що поширюють інформацію про безпеку онлайн, залучення ЗМІ для поширення необхідної інформації.

4. Законодавство в інформаційній сфері забезпечують з мінімальними ризиками діяльність електронного уряду.

5. Міністерство внутрішніх справ та Міністерство оборони реалізують безпеку додатків (поширення ідентифікаційних карт (*ID cards*), застосування телематичних служб в мережах,якими користуються органи державної влади.

Державну стратегію безпеки в інформаційній сфері Естонія затвердила 8 травня 2008 року.[12]. Відповідно до якої, основними напрямками інформаційної політики держави визнано: аналіз державної критичної інфраструктури, реалізація запобіжних та попереджувальних механізмів з протидії кібератакам, встановлення компетенцій органів державної влади в сфері керування кібербезпекою, покращення правового фундаменту, збільшення інформації у громадян Естонії щодо кіберзагроз, їх протидії, сприяння міжнародній прів праці, налагодження зв'язків між державами.

Основними принципами національної стратегії кібербезпеки є:

- входження питання кібербезпеки як основного елемента системи національної безпеки;

- забезпечення діалогу між усіма органами державної влади щодо інформаційної безпеки;

- розповсюдження інформації серед громадян Естонії з приводу можливих небезпек у кіберпросторі і відповідної реакції та протидії ним;

- співпраця із міжнародними установами з метою забезпечення кібербезпеки Естонії;

- захист прав людини і відомостей про особу.

Стратегічними цілями Естонії щодо кібербезпеки виступають:

1. забезпечення ефективного механізму заходів у сфері безпеки інформаційного простору;

2. розповсюдження інформації серед громадян країни щодо інформаційної безпеки;

3. створення правового фундаменту для здійснення кібербезпеки;

4. посилення ролі Естонії у якості країни-лідера на міжнародній арені щодо кібербезпеки.

В Естонії першочергове значення має захист критичної інформаційної інфраструктури, створення ефективних заходів безпеки і налагодження співпраці між усіма державними органами.

Захист критичної інформаційної інфраструктури в Естонії полягає в:

встановлення чіткого переліку послуг, яким необхідна критична інформаційна інфраструктура;

- встановлення взаємозв'язків критичної інфраструктури і критичної інформаційної інфраструктури;

- створення системи аналізу та перевірки інформаційних систем критичної інфраструктури;

- моніторинг кіберпростору держави задля створення ефективних превентивних заходів та контрзаходів щодо забезпечення національної кібербезпеки Естонії.

Розробка та впровадження системи заходів безпеки передбачає визначення додаткових засобів безпеки інформаційних систем; визначення мінімального рівня функціональності інформаційної інфраструктури та забезпечення цього рівня функціонування у кризовій ситуації; визначення заходів протидії у надзвичайній ситуації, якщо на об'єкти критичної інфраструктури здійснено атаку; вироблення економічно прийнятних й оптимальних методів забезпечення інформаційної безпеки; розробка методів тестування для засобів безпеки; вдосконалення систем ідентифікації та моніторингу електромагнітного впливу на критичну інфраструктуру; зміцнення інфраструктури Інтернет; підвищення безпеки систем контролю (наприклад, SCADA (Система управління і збору даних) - автоматизована система управління і контролю, що використовуються в промисловості); перевірка рівня безпеки об'єктів критичної інформаційної інфраструктури з точки зору електромагнітних впливів.

Контроль за впровадженням заходів безпеки для критичної інфраструктури здійснює Міністерство внутрішніх справ та Міністерство економіки і комунікацій у співробітництві з іншими міністерствами, що відповідають за різні сектори критичної інфраструктури.

Для зміцнення організаційного співробітництва передбачено реалізацію таких заходів:

- створення Ради з кібербезпеки в Комітеті з питань безпеки естонського уряду, уповноваженого втілювати у життя Стратегію кібербезпеки;
- визначення повноважень структурного підрозділу Міністерства економіки і комунікацій, що відповідає за безпеку державних інформаційних систем;
- вдосконалення методів оцінки ризиків, розроблених міністерствами та використання цих методів в сфері кібербезпеки;
- створення експертної робочої групи (яка надаватиме професійні поради Раді з кібербезпеки), уповноваженої виявляти прогалини в

інформаційній безпеці, визначати необхідні ресурси для оновлення безпекових заходів та обмінюватися оперативною інформацією;

- формулювання пропозицій для внесення поправок у національне і міжнародне законодавство;

- координація заходів щодо підвищення обізнаності в сфері кібербезпеки та визначення органу, відповідального за проведення цих заходів.

Основними способами підвищення компетентності в сфері кібербезпеки визначено організацію навчань (тренінгів) з питань кібербезпеки та проведення досліджень. Сюди відноситься, зокрема, встановлення вимог до знань в сфері інформаційної безпеки та кіберзахисту для робітників державного і приватного секторів та впровадження відповідної системи оцінювання; підвищення рівня підготовленості до кризових ситуацій в державному та приватному секторах; створення в Естонії під егідою НАТО Центру експертизи з питань кооперативної кібер-оборони (NATO Cooperative Cyber Defence Centre of Excellence).

Діяльність щодо правового регулювання сфери кібербезпеки включає розробку правових визначень кібербезпеки та кіберзлочину; впровадження законодавства щодо питань кібербезпеки, включаючи запровадження обов'язкових заходів та стандартів безпеки і встановлення мінімальних вимог до безпеки інформаційних систем; започаткування ініціатив у законотворчій діяльності на міжнародному рівні тощо.

Діяльність щодо зміцнення міжнародної співпраці з питань кібербезпеки передбачає винесення проблем кібербезпеки на міжнародний «порядок денний»; сприяння ратифікації країнами Конвенції Ради Європи про кібезлочинність; обговорення проблем кібербезпеки на конференціях, семінарах та форумах; надання підтримки міжнародним корпораціям, асоціаціям, дослідницьким інститутам та неурядовим організаціям, які займаються проблемами кібербезпеки; просування кращої практики в сфері

кібербезпеки на міжнародному рівні; направлення представників Естонії до експертних груп міжнародних організацій, задіяних в сфері кібербезпеки.

Важливу роль у вирішенні проблем інформаційної безпеки в Естонії відіграє Естонська інспекція захисту даних. Це установа державного нагляду, основними напрямами діяльності якої є [13]:

- надання правової допомоги і здійснення контролю (надання порад, роз'яснення, розгляд скарг, здійснення перевірок, участь у діяльності європейських організацій з питань захисту даних);
- створення баз даних державного сектору;
- реєстрація обробки конфіденційних персональних даних;
- авторизація обробки даних (авторизація обробки даних для наукових або статистичних цілей без згоди людини, авторизація передачі персональних даних з недостатнім рівнем захисту до зарубіжних країн);
- здійснення адміністративного примусу та виконання наказів щодо правової відповідальності тощо.

Інспекція здійснює нагляд за власниками інформації та особами, які обробляють персональні дані. Крім приватного сектору, діяльність Інспекції охоплює усі державні установи. У випадках, коли інтереси по захисту персональних даних протирічать інтересам щодо розголошення інформації, роль Інспекції полягає у тлумаченні та застосуванні правових норм так, щоб забезпечити збалансований захист обох благ.

З 2006 року в Естонії працює Комп'ютерна група швидкого реагування (CERT Estonia) – організація, відповідальна за управління безпековими інцидентами в національних комп'ютерних мережах (точніше, мережах домену «.ee»). Організація надає допомогу естонським Інтернет-користувачам у реалізації превентивних заходів, з метою мінімізації шкоди від безпекових інцидентів та у реагуванні на загрози безпеці. Обсяг підтримки, що надається CERT Estonia, залежить від типу та серйозності

безпекового інциденту, від кількості потенційно постраждалих користувачів та наявних в організації ресурсів.

Комп'ютерною групою швидкого реагування Естонії надаються такі послуги:

- управління інцидентом – прийняття повідомлень про інцидент, пріоритизація інцидентів залежно від рівня серйозності; аналіз інциденту; надання допомоги у реагуванні на інцидент; координація дій з реагування на інцидент;

- інформування і попередження – інформування користувачів про атаки, віруси, «хробаків», «троянів» в мережах домену першого рівня «.ee» та сповіщення про уразливі місця, виявлені у найбільш популярних в Естонії системах і додатках.

CERT Estonia не надає послуг кінцевим користувачам, тому у разі безпекового інциденту користувачі мають звертатися до системних адміністраторів їхнього Інтернет-провайдеру, до мережевих адміністраторів або до служби підтримки споживачів.

В Естонії також функціонує декілька неурядових організацій, які роблять свій внесок у зміцнення інформаційної безпеки держави. Серед них - Фонд Look@World та Центр сертифікації.

У 2001 році десять провідних компаній Естонії створили Фонд Look@World з метою підвищення кількості Інтернет-користувачів в країні. Фондом реалізовано такі проекти, як тренінги з користування комп'ютерами та мережею Інтернет для 100,000 громадян, створення середовища eSchool, відкриття 500 пунктів доступу до мережі Інтернет.

23 травня 2006 року основні учасники Фонду Look@World та Міністерство економіки і комунікацій Естонії підписали договір про співпрацю щодо започаткування загальнонаціональної ініціативи під назвою «Computer Protection 2009». Мета проекту – перетворити Естонію на країну з найбільш безпечним інформаційним суспільством у світі до 2009 року.

Ініціатива відома під назвою «Look@World 2». Впродовж трьох років партнери Фонду Hansapank, EMT, SEB Eesti Ühispank та Elion фінансують ініціативу у розмірі 3.83 мільйонів євро.

За договором, сторони зобов'язуються забезпечити стійкий розвиток е-послуг та ІТ-рішень, що надаються державою та приватним сектором; дати можливість користувачам е-послуг активно брати участь у захисті інформаційного суспільства, зберігаючи при цьому стабільне середовище та довіру до цих послуг; сприяти заходам із підвищення обізнаності та вдосконалення навичок, пов'язаних із ІТ-безпекою; створити умови для підвищення простоти, доступності та зручності у користуванні апаратних засобів та програмного забезпечення.

Сторони домовилися об'єднати зусилля для забезпечення розробки і впровадження додатків на базі ідентифікаційної картки (ID card) та сучасної криптографічної системи з відкритим ключем.

Згідно з договором внесок Міністерства економіки і комунікацій Естонії у реалізацію ініціативи полягає у наступному:

- надання пріоритетного значення питанням інформаційної безпеки під час розробки стратегій та законодавства стосовно інформаційного суспільства і забезпечення ефективної діяльності Комп'ютерної групи швидкого реагування Естонії;

- використання рішень, що враховують можливості ідентифікаційної картки у розвитку нових безпечних публічних е-послуг та у функціонуванні державної адміністрації;

- сприяння діалогу з питань безпеки мережі Інтернет між державним і приватним секторами;

- пошук і обмін інформацією про програми ЄС, спрямовані на розвиток безпечного інформаційного суспільства;

- поширення досвіду Естонії в сфері електронної ідентифікації в країнах ЄС та полегшення обміну кращим досвідом з іншими країнами;

- участь у розробці та просуванні системи показників безпеки Інтернет та реалізації аналітичних досліджень щодо використання ідентифікаційних карток та е-послуг.

Діяльність Фонду Look@World в рамках ініціативи «Computer Protection 2009» полягає у наступному:

- просування і пріоритетний розвиток ідентифікаційних карток;

- інтеграція ідентифікаційної картки та інших механізмів ідентифікації на базі технології PKI (Public Key Infrastructure) у свої послуги та забезпечення максимального використання цифрового підпису у бізнес-процесах;

- інвестування в інфраструктуру та подібні послуги;

- проведення тренінгів та надання інформації естонським громадянам щодо користування ідентифікаційною карткою в електронних системах;

- розробка і впровадження нових послуг, що базуються на ID-картках;

- надання консультацій підприємствам та установам щодо розвитку послуг на базі ідентифікаційних карток;

- реалізація заходів щодо підвищення громадської обізнаності в сфері інформаційної безпеки, зокрема створення і підтримку порталу, присвяченого безпеці інформаційних технологій;

- поширення інформації про безпеку інформаційних технологій через засоби інформації;

- розробка показників Інтернет-безпеки та їхнє просування.

З метою інформування громадськості про ідентифікаційну картку як найбільш простий та безпечний механізм самозахисту під час використання е-послуг створено сайт http://koolitus.id.ee, на якому пояснюється, чому необхідна ідентифікаційна картка, як її отримати, як нею користуватися, як зробити електронний підпис тощо. Інформація доступна естонською та російською мовою. Крім того, створено сайт, де розміщено корисну інформацію з питань безпеки інформаційних технологій: www.arvutikaitse.ee (естонська версія), www.infosecurity.ee (російська версія).

У лютому 2001 року двома провідними банками Естонії Hansapank і SEB спільно з двома телекомунікаційними компаніями Elion і EMT створено Центр сертифікації. Це єдина установа в Естонії, яка видає сертифікати на аутентифікацію та електронний підпис для ID-карток. Основна функція Центру – забезпечення надійності та цілісності електронної інфраструктури для ідентифікаційних карток. Центр не лише видає сертифікати на ідентифікаційні картки, але й надає послуги, пов'язані із юридичною дієвістю сертифікатів та використанням електронних підписів. Послугами Центру користуються естонські банки, судові органи і нотаріуси, правоохоронні органи, Республіки Латвія та Литва та багато інших [15].

Центром сертифікації та його партнерами створено безпечну, надійну й зручну технологію DigiDoc, яка дозволяє створювати електронні підписи у будь-яких формах комунікації. Технологія, яка стала стандартом в Естонії, використовується здебільшого державним сектором (судами, урядом, органами місцевого самоврядування, банками тощо).

Механізми захисту інформаційного простору України можна виробити, проаналізувавши ефективну модель інформаційної безпеки, що застосовується у Великобританії, де правоохоронні органи постійно співпрацюють із ІКТ-провайдерами через конвергентний орган Великобританії в інформаційній сфері Ofcom [92]. За настановами Ofcom 4 найбільших провайдери (послуги яких охоплюють 95 % домогосподарств) застосовують фільтри для блокування будь-якого контенту. Задля забезпечення безпеки в інформаційній сфері, потрібно активно співпрацювати правоохоронним органам, провайдерам Інтернет-послуг та громадським організаціям, державним органам, що покликані забезпечити інформаційну безпеку в межах організації Internet Watch Foundation, що дозволяє припинити розповсюдження протиправного контенту, який розповсюджується за допомогою соціальних мереж (Facebook та ін.) та Google. В інформаційній сфері Великобританія використовує безпекові та

судові органи. Наприклад, публікація незаконних повідомлень у соціальних мережах у Великобританії є достатньою підставою для порушення кримінальної справи та висунення обвинувачення [91].

В цілому, видається цікавим звернутися до досвіду європейських країн в контексті інформаційної безпеки. Так, Уряд Великобританії почав займатися проблемами захисту інформації раніше інших європейських держав. З одного боку це добре, оскільки дозволило країні накопичити достатньо солідний досвід в цій області. Однак, якщо поглянути на це питання з іншого боку, то з'ясується, що вся система захисту інформації Великобританії має серйозні недоліки. Раніше основною метою вважалася безпека країни. Відповідно, всі органи, які повинні були захищати інформацію, створювалися урядом і були підпорядковані йому ж або відповідним спецслужбам. Відповідно, а забезпечення безпеки персональних і комерційних даних виявилося другорядним завданням. І це проявляється всюди.

Взяти хоча б правове забезпечення захисту інформації в Великобританії. Основою є закони «Про державні документи» і «Про державну таємницю». Для забезпечення безпеки решти інформації використовується кримінальний кодекс і деякі інші правові акти. Окремо варто згадати про захист комерційної таємниці. Справа в тому, що про це кожна організація повинна піклуватися це самостійно, використовуючи спеціальні договори, які укладаються з працівниками перед наданням їм доступу до даних.

Як ми вже говорили, всі організації, які контролюють захист інформації в Великобританії, підпорядковані уряду. Крім того, всі великі компанії мають власні служби безпеки. Середній бізнес часто користується послугами приватних фірм, що реалізують і підтримують корпоративні системи захисту інформації. Ці служби часто об'єднують зусилля і співпрацюють один з одним і з державними структурами. Фактично, на їх плечах лежить вся тяжкість боротьби з недобросовісною конкуренцією та промисловим шпигунством.

Ще однією проблемою організації системи захисту інформації в Великобританії є консервативність. Розроблена колись система залишається незмінною вже досить давно. Тим часом в області інформаційних технологій все змінюється дуже швидко, так що періодично виникає необхідність певної корекції органів захисту даних.

Німеччина - одна з найбільш «прогресивних» в області інформаційної безпеки країн Західної Європи. Вона володіє розвиненою структурою органів, що піклуються про захист різних видів таємниць. Первинним завданням цих структур був захист від промислового шпигунства і охорона державних секретів. Вперше організації, що займаються цими питаннями, почали створюватися аж в 19-м столітті. З тих пір, звичайно ж, змінилося дуже багато чого. Однак і сьогодні у всіх компаніях, в яких працює хоча б десяток людей, один із співробітників призначається уповноваженим із захисту інформації. В його обов'язки входить посильну протистояння всім злочинам в комп'ютерній сфері, а також тісна співпраця з відповідними відділами правоохоронних органів. Природно, у великих компаніях, на відміну від невеликих фірм, уповноважений займається тільки захистом інформації, а у нього в підпорядкуванні знаходиться ціла група співробітників.

До 1970 року в Німеччині (тобто, в ФРН) ніхто не займався питаннями захисту персональних даних. Однак з тих пір все змінилося. Сьогодні кожен громадянин Німеччини має право на захист особистої інформації. В принципі, це прописано і в законодавстві практично всіх інших країн. Але німці не обмежилися однією тільки записом на папері, а взялися реалізувати цей вислів на практиці. І у них все вийшло. Для контролю захисту особистої інформації була створена спеціальна структура з уповноважених із захисту персональної таємниці. Її головна особливість - незалежність від будь-яких державних органів. До завдань уповноважених входить перевірка скарг громадян про незаконне використання їх особистих даних. Причому, що

цікаво, більшість претензій пред'являється якраз державним структурам, в тому числі, і правоохоронним органом. Таким чином, незалежність уповноважених - це гарантія свободи громадян і надійний захист від свавілля з боку держави.

Крім того, дуже велику користь приносить федеральне відомство по забезпеченню безпеки в сфері інформаційної техніки. У завдання цієї організації входить координування роботи інших структур щодо захисту даних, сертифікація і стандартизація засобів безпеки. Крім того, відомство займається пропагандою необхідності захисту даних, а також надає консультаційні послуги в цій галузі. Отже, інформаційна безпека в ЄС розглядається, насамперед, як стан інформаційних мереж і систем, що забезпечує достатній рівень захисту інформації та належний рівень протидії зовнішнім негативним впливам на інформаційну безпеку. Пріоритетним напрямком розвитку політики країн ЄС в інформаційній сфері є створення і ефективна реалізація програм та технічних засобів, що забезпечують підтримку належного рівня захисту інформаційно-комунікаційних технологій. Також основним акцентом політики в інформаційній сфері є створення правового фундаменту інформаційної безпеки, що включає розробку нормативно-правових актів, що регулюють питання визначення вичерпного переліку злочинів, пов’язаних з інформаційними технологіями та кримінальну відповідальність за їх здійснення. Інформаційна безпека громадян є іншим пріоритетом політики ЄС. Забезпечення інформаційної безпеки громадян реалізується за допомогою розповсюдження інформації про ризики і загрози, пов’язані із інформаційними технологіями, дієві механізми захисту інформаційних систем/мереж громадян від атак та небажаних впливів. До цього можна віднести протидіб кібератакам, захист персональних даних, моніторинг і виявлення шкідливого контенту в мережі Інтернет тощо.

Стратегія кібербезпеки Канади датується в 2010 р. і будується на трьох основних принципах:

- забезпечення державних систем;

- співробітництво для забезпечення життєво важливих кібер систем за межами федерального уряду.

- убезпечити канадців в Інтернеті.

Перший компонент спрямований на встановлення чітких функцій і обов'язків, з метою зміцнення безпеки федеральних кібер-систем і підвищення рівня інформованості кібер безпеки в усьому уряді.

Другий компонент охоплює цілий ряд партнерських ініціатив з провінцій і територій за участю приватного сектора і найважливіших секторів інфраструктури.

І, нарешті, третя опора охоплює боротьбу з кіберзлочинністю і захисту канадських громадян в Інтернеті. Питання права на приватне життя, зокрема, розглядаються в цій «рубриці».

В цілому, зазначені стратегії інформаційної безпеки держав по всьому світі наділені наступними спільними рисами:

- Визначення структури управління для кібер-безпеки.

- Визначення відповідного механізму (часто державно-приватного партнерства), яка дозволяє всім державним та приватним зацікавленим сторонам обговорювати та узгоджувати на різних політичних і нормативних рівнях кібер безпеки питання.

- Формулювання необхідних політичних та нормативних заходів та чітко визначення ролей, обов'язків і прав приватного і державного сектора (наприклад, нові правові рамки для боротьби з кіберзлочинністю, обов'язкова звітність про інциденти, мінімальні заходи безпеки і керівні принципи, нові правила закупівель). Наприклад, стратегія Словаччини визначає необхідність визначення юридичних меж для захисту кіберпростору (дивитись в роботі).

- Встановлення цілей і засобів для розвитку національного потенціалу і необхідної правової бази брати участь у міжнародних зусиллях щодо зменшення наслідків кіберзлочинності. Низка стратегій містить особливий акцент на боротьбі з кіберзлочинністю.

- Розробка або поліпшення забезпечення готовності, планів реагування та відновлення, а також заходів щодо захисту (наприклад, національні плани дій в надзвичайних ситуаціях, кібер вправи, і розуміння ситуації).

- Визначення системного і комплексного підходу до національного управління ризиками (наприклад, обміну інформацією за довірою та національні реєстри ризиків).

Як бачимо, не всі стратегії окремо прописують питання впливу на населення, за діяння громадськості в формулюванні інформаційної безпеки або окремо прописують соціум як суб'єкт або об'єкт впливу. На нашу думку, виходячи з останніх викриків і загроз, варто або внести окремі зміни в національні стратегії або навіть розробити і прийняти нову стратегію/доктрину.

Виникає питання, як саме підготувати правильну стратегію для країни з низьким розвитком національної безпеки в сфері інформації.

Перш за все, необхідно підготувати матеріали, технічні та фінансові ресурси для протидії інцидентам в області безпеки, а також в подальшому формувати спеціалізованої організації по боротьбі з комп'ютерною злочинністю та забезпечити взаємне співробітництво, обмін інформацією та досвідом на національному рівні з посиланнями до загальноєвропейського середовища. Такі установи будуть виконувати завдання, брати участь у виконанні завдань, виробляти план дій і т.д. Також слід нарощувати кадровий потенціал, який в даному випадку буде навчатися за рахунок співпраці з іноземними державами.

Таким чином, маючи стратегію, уряд країни може роздавати компетенції структурам, які будуть працювати у сфері інформаційної безпеки держави.

Також важливою формою протидії небезпеці в інформаційному просторі є належне технічне устаткування, оскільки сьогодні атаки ворогів перемістилися з наземної території в кіберпростір.

Збір, отримання, передача та розшифрування інформації сьогодні напряму залежить від того, якою технікою та інноваціями користується держава. Звичайно, не слід забувати, що важливо не забувати підтримувати кваліфікацію працівників, оскільки маючи навіть найсучасніше обладнання та програмне забезпечення, якщо працівники певних структур не будуть знати як ним користуватись, кошти, які були витраченими на його розробку чи купівлю будуть марними.

Розробки програм, які регулюють інформаційний простір, давно вийшли за рамки держави. Це означає, що програмісти фрілансери сьогодні з радістю напишуть програму, яка, наприклад буде блокувати в рамках національної безпеки та безпеки інформаційного простору певні шкідливі віруси, повідомлення чи інформацію. Такими розробками радо користуються уряди країн для регулювання інфопростору в країні.

Велика кількість стандартів та специфікацій, що не узгоджуються між собою призводить до поділу ринку та необхідності дійти до уніфікованого підходу. Основним завданням виступає гармонізація, удосконалення та уніфікація усіх стандартів.

Підсумовуючи та аналізуючи вищенаведені дані, особливості, досвід та практику різних держав, маючи на увазі практику та особливий досвід України (мова про протидію України інформаційній війні в контексті протидії російській агресії детальніше розглядатиметься автором в наступному підрозділі), автор пропонує специфічні критерії, які на його думку, мають стати наріжними в роботі держави на напрямку інформаційної безпеки (див.таб.). особливий акцент автора – «обігравання» соціокомунікаційного виміру при забезпеченні інформаційної безпеки

держави як ключового в контексті сучасних подій в Україні та загальних світових тенденцій.

Таблиця

ілюстрації забезпечення державами національної і громадської безпеки в інформаційному просторі на рівні стратегій (доктрин) інформаційної безпеки з врахуванням соціокомунікаційного аспекту

Критерії	Держави									
	США	**Канада**	**Фінляндія**	**Німеччина**	**Велика Британія**	**Естонія**	**Японія**	**Австралія**	**РФ**	**Україна**
Наявність конституційних прав і свобод громадян в інформаційній сфері	+	+	+	+	+	+	+	+	+	+
Закріплення та реалізація права на приватне життя (кореспонденція, комунікація)	+ -	+	+	+	+	+	+	+	+	+
Захист інформаційної інфраструктури	+	+	+	+	+	+	+	+	+-	+-
Протидія кіберзлочинності	+	+	+	+	+	+	+	+	+-	-+
Наявність окремого органу для відання питанням інформаційної безпеки	+	+	+	+	+	+	+	+	-	+

Участь держави у регіональних та міжнародних проектах/альянсах/організаціях	+	+	+	+	+	+	+	+	+	-+
Віднесення фізичних та юридичних осіб до *суб'єктів* потенційних загроз безпеці держави	+	+	+	+	+	+	+	+	+-	-+
Віднесення фізичних та юридичних до *об'єктів* потенційних загроз безпеці держави	+-	+-	-	-	-	-	-	-	-	-
Робота держави над виявленням та протидія «шумам» в комунікаційному процесі за участю громадськості	+	-	-	-	-	-	-	-	-	-
Протидія пропаганді	+-	-	-	-	-	-	-	-	-	-
Робота над захистом та просуванням національних цінностей та ідей	+	+	+	+-	+	+-	+-	+	-	-
Активне використання публічної дипломатії	+	+	+	+	+	+	+	+	+-	-+

Таким чином, як свідчать дані, наведені у табличці, можна говорити, що загалом типовим для усіх країн світу є вироблення механізмів забезпечення інформаційної безпеки держави у соціально-комунікаційному плані такими засобами: забезпеченням балансу інтересів особи, суспільства та держави; системне вироблення концепції держави у сфері національної безпеки і соціокомунаційної сфери загалом «набирає обертів», однак, потребує вироблення окремими державами певних акцентів на цьому напрямків; комплексний підхід – налагодження співпраці не тільки між усіма державними органами, що забезпечують безпеку у державі – наприклад Міністерством закордонних справ, Міністерством інформаційної політики та Міністерством оборони (які, зокрема, представлені в Україні), активна співпраця із науковими інституціями та науково-дослідними інститутами, але й інтеграція з міжнародними системами безпеки, участь у розробці й послідовна імплементація уніфікованих правила забезпечення інформаційної безпеки на різних міжнародних форумах. Зокрема, забезпечення інформаційної безпеки держави залежить також від ефективності публічної демократії, налагодження зв'язків між державами, покращення співпраці шляхом проведення міжнародних конференції, а так просування позитивного іміджу держави за кордоном, спрямування її представлення в «найкращому світлі», орієнтоване на пересічних громадян, які в перспективі мають бути «іноземними адвокатами» держави.

3.3 Соціальнокомунікаційна модель інформаційної безпеки у структурі національної безпеки України

Відповідно до Концепції національної безпеки, національна безпека України - це стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз. Таким чином, діяльність у сфері національної безпеки спрямована на захист життєво важливих інтересів особи, суспільства і держави. На підставі цих інтересів визначають комплекс загроз, на запобігання яких і спрямована політика національної безпеки.

Звідси зрозуміло, що подолати будь-яку систему безпеки, зокрема національну, можливо трьома основними способами:

- посилити тиск за напрямами, проти яких спрямована система безпеки;
- знайти та створити такі загрози, проти яких система безпеки не спрацює;
- змінити систему інтересів, а відповідно і комплекс загроз, щоб нейтралізувати дії системи безпеки [93].

Система забезпечення національної безпеки не є самостійним об'єктом інтересу з боку зовнішніх або внутрішніх загроз. Потужність системи національної безпеки у спроможності протистояти загрозам [93].

«Національна безпека - це захист інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз. Національна безпека включає у себе усі сфери життя суспільства як аспекти забезпечення національної безпеки.

Коли аналізують національну безпеку, враховують, що вона досягається шляхом проведення чітко визначеної державної політики відповідно до прийнятих стратегій, концепцій і програм у всіх сферах суспільного життя, і інформаційній сфері зокрема. Національна безпека починається там де є загрози і упередженості з проблем національного розвитку, існування окремо взятої держави, країни чи суспільства» [94]. В цілому, стратегія національної безпеки України комплексно затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року

«Про Стратегію національної безпеки України», і передбачає визнання факту, що «Росія окупувала частину території України - Автономну Республіку Крим і місто Севастополь, розв'язала воєнну агресію на Сході України та намагається зруйнувати єдність демократичного світу, ревізувати світовий порядок, що сформувався після закінчення Другої світової війни, підірвати основи міжнародної безпеки та міжнародного права, уможливити безкарне застосування сили на міжнародній арені» усіма способами, а кожним з них і виступає у сучасному світі пропаганда.

Методи забезпечення національної безпеки України як окремої держави зумовлюються пріоритетністю її національних інтересів, необхідністю своєчасного вжиття заходів, що відповідають масштабам загроз державним інтересам. А зміст державної політики в інформаційній сфері визначається прийнятими на законодавчому рівні стратегіями і принципами забезпечення національної безпеки. У кожній державі діють унікальні принципи безпеки в інформаційній безпеці.

Основною стратегічною метою національної безпеки України, як і кожної країни, є забезпечення захисту: природи як сфери існування людини; людини (її прав і свобод); соціальних та національних груп - їх статусу, суспільства; держави (її суверенітету, територіальної цілісності). Усі сфери життя суспільства не можуть ефективно розвиватись без відповідного інформаційного поля, «інформаційної» політики.

Стратегічна мета національної безпеки полягає у постійному вдосконаленні системи забезпечення національної безпеки в інформаційній сфері. Вирішення проблем національної безпеки України полягає в захисті власних національних інтересів від держав, юридичних і фізичних осіб, які намагаються забезпечити своє існування і розвиток агресивними методами за допомогою інформаційних технологій. Самостійна суверенна держава не може існувати без забезпечення власної інформаційної безпеки.

Як зазначає Е.А. Позняков, «якщо по відношенню до власної держави нація часто являє собою роз'єднане ціле, то стосовно зовнішнього світу та інших держав - єдине ціле. Відповідно і національний інтерес набуває значення інтересу нації загалом і, головним чином, відносно зовнішнього світу» [94].

Національна безпека і її складова - інформаційна безпека, являють собою складний суспільний процес, що постійно розвивається, залежно від стану і характеру суспільства, суспільних відносин, діючих концепцій, існування протилежних точок зору. Однак, чітко прослідковується взаємозалежність: чим більш розвиненим є суспільство, тим стабільнішою, стійкішою до загроз є система національної безпеки в інформаційній сфері.

Особливості національної безпеки держави розкривають зміст функціонування суспільства і держави, визначають сучасний стан і тенденції до змін суспільства.

Питання інформаційної безпеки як складової національної безпеки викликано розвитком інформаційних технологій, техніки та збільшенням кількості конфліктів між державами. Ще за часів так званої «холодної війни» інформація, та інформаційні системи залишилися дієвим інструментом впливу одних держав і народів на інші. Щодо сьогодення, то інформація, інформаційні засоби є потужним джерелом розвитку держав, їх перетворення на інформаційні держави та суспільства. М.М. Нетрубач вважає, що так зване інформаційне суспільство, до якого прагне багато країн, може бути визначене саме як «суспільство, в якому предметом праці більшості є знання та інформація, а знаряддям праці - інформаційні технології» [94].

Для вироблення необхідної моделі інформаційної безпеки необхідно визначити загрози інформаційній безпеці, що проаналізовано у попередньому розділі дослідження. На разі вдалось виявити відсутність єдності у поглядах, що стосуються класифікації відповідних загроз як на нормативно-правовому, так і на науковому рівнях. Доктрина інформаційної безпеки України визначає

основні реальні та потенційні загрози інформаційній безпеці України класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері, внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, в екологічній сфері.

Все більшого значення набуває питання координації враховуючи те, що, на відміну від більшості галузей, саме у сфері інформаційних технологій постійно змінюється термінологія, змінюються методи та засоби передачі, отримання, обробки та зберігання інформації, що призводить до того, що одне й те саме поняття описується завдяки різним термінам. Наприклад, під поняттям «інформаційні війни» фахівці технічних галузей знань розуміють порушення електронної інфраструктури суспільства (у розвинених країнах – мережі державних та фінансових установ, таких як управління транспортом, військові системи, що піддаються атакам кібертерористів). У разі, коли здійснення терористичного акту буде поєднано з атакою на інформаційну систему рятувальних служб, медичних закладів чи правоохоронних органів, збитки від даних дій будуть значними. Дані загрози призвели до появи у системі національної безпеки спеціальних силових підрозділів, що володіють інформаційною зброєю та необхідними методами захисту.

Працівники засобів масової інформації під «інформаційними війнами» розуміють нав’язування певної суспільної думки за допомогою засобів масової інформації, у тому числі через електронні видання та соціальні мережі.

Якщо на побутовому рівні різне тлумачення визначень розуміють і аналізують виходячи з контексту повідомлення, то у правозастосуванні понятійна невизначеність призводить до нівелювання правової основи.

Реалізацію основної мети держави - забезпечення інформаційної безпеки – в Україні пришвидшило створення Міжвідомчої комісії згідно із Указом Президента України «Про Міжвідомчу комісію з питань інформаційної

політики та інформаційної безпеки при Раді національної безпеки і оборони України» від 22 січня 2002 р. № 63/2002, яку очолює Секретар Ради національної безпеки і оборони України і основним завданням якої стала координація діяльності усіх органів державно влади у сфері інформаційної безпеки.

Концепція інформаційної безпеки України таким чином поєднує систематизацію питань, визначення методів та засобів інтересів особистості, суспільства, держави в інформаційній сфері, створення засад для формування державної політики інформаційної безпеки, розвиток інформаційного простору країни. Відповідно, метою забезпечення інформаційної безпеки в Україні є створення захищеного інформаційного простору, захист національних інтересів України в умовах формування світових інформаційних мереж, захист економічного потенціалу держави від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ та держави на отримання достовірної інформації.

Основні задачі забезпечення інформаційної безпеки:

• виявлення джерел загроз інформаційній безпеці;

• розробка державної політики забезпечення інформаційної безпеки та комплексу заходів її реалізації;

• створення нормативно-правових засад забезпечення інформаційної безпеки;

• вдосконалення системи забезпечення інформаційної безпеки;

• забезпечення участі України в процесах створення і використання глобальних інформаційних мереж та систем [95].

Протидія інформаційній агресії та цілеспрямованим кампаніям у іноземних ЗМІ проти України є одним з першочергових елементів гарантування національної безпеки України у зовнішньому вимірі. Інформаційні війни стали поширеним інструментом здобування політико-економічних інтересів держав, котрі прагнуть посилити свій вплив на

формування громадської думки в Україні з метою її подальшого використання для реалізації власних зовнішньополітичних стратегій.

Україна є об'єктом потужної спланованої інформаційної агресії Росії, а тому має враховувати усі вище написані аспекти при розробці нової більш ефективної концепції інформаційної безпеки, яка має врахувати сучасні тенденції розвитку соціальних мереж, механізмів ведення інформаційних воєн та розвиток інформаційних технологій.

Варто на загальнодержавному рівні надавати ресурсне та організаційно-технічне сприяння телерадіокомпаніям та друкованим ЗМІ України, котрі своєю діяльністю сприяють поширенню позитивної інформації про нашу державу у європейському та світовому інформаційному просторі.

Так, діяльність держави та ЗМІ мають спрямовуватись на розширення присутності «української тематики» у міжнародному інформаційному просторі, що стало б протидією деструктивним кампаніям у міжнародному інформаційному середовищі, спрямованим проти України [96]. Цей крок є також позитивним у напряму зміцнення інформаційного сегменту національної безпеки нашої держави, котрий наразі перебуває під постійним агресивним впливом певних держав, де інформація про Україну подається упереджено, не об'єктивно та носить переважно дискредитаційний характер. Відсутність належної симетричної реакції з боку нашої держави на подібні випади провокує, у свою чергу, посилення ступеню тиску на українське суспільство, особливо з огляду на те, що телерадіокомпанії деяких прикордонних держав мають право поширювати своє мовлення на українську територію.

Для інформаційної безпеки України, принципового значення набувають відносини України з окремими державами, континентами - передусім Європою та окремими альянсами і організаціями.

Серед актуальних загроз державі Україна агресивними діями Російської Федерації визначено «інформаційно-психологічну війну, приниження

української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу». Фактично на державному рівні визнано інформаційну війну, що проводить Росія проти України у період з 2013 по 2015 роки. Серед основних національних загроз визначено «Загрози кібербезпеці і безпеці інформаційних ресурсів, що розшифровуються як «уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом».

Таким чином, до 2020 року у своїй стратегії національної безпеки Україна як основними пріоритетними сферами визначила: забезпечення інформаційної безпеки та забезпечення кібербезпеки і безпеки інформаційних ресурсів. Пріоритетами забезпечення інформаційної безпеки визначено 1) забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; 2) створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; 3) протидію інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; 4) розробку і реалізацію скоординованої інформаційної політики органів державної влади; 5) виявлення суб'єктів українського інформаційного простору, що створені або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; 6) створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав - членів НАТО; 7) удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу. Пріоритетами забезпечення кібербезпеки і безпеки інформаційних

ресурсів на державному рівні виступають: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, посилення співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки» [97].

Фундаментальну стратегію національної безпеки і в інформаційній сфері і рекомендації для органів державної влади по їх втіленню у життя розробляє Національний інститут стратегічних досліджень при Президентові України. В їх аналітичній записці мова йде не про інформаційну війну Російської Федерації, а гібридну з використанням інформаційних спецоперацій та пропаганди російською стороною. Доцільним видається проаналізувати на прикладі даної інформаційної війни вплив однієї держави за допомогою механізму пропаганди на ескалацію насильства у зоні підконтрольній терористам на території іншої держави (у нашому варіанті - ДНР/ЛНР) та забезпечення інформаційної безпеки як складової національної безпеки держави.

Єдиного визначення пропаганди не існує, однак у Міжнародній конвенції про використання радіомовлення в інтересах миру визначено її цілі як «дії, спрямовані на підбурювання населення будь-якої території до дій, що несумісні із внутрішнім порядком чи безпекою будь-якої території», Конвенція була підписана СРСР у 1983 році і є чинним документом і у Російській Федерації [97, 98]. Для того щоб позбавити її виключно емоційного характеру, потрібно проаналізувати наявні факти її застосування. Так, відомі приклади відповідальності засобів масової інформації за розпалювання ворожнечі, наприклад, за вироком Міжнародного кримінального трибуналу по Руанді щодо засновників RTLM (Radio Television Libre des Mille Collines, «Радіо Тисячі Пагорбів») за насильство з боку груп ополченців, що спричинено радіотрансляцією програм радіо: «Інтерахамве [збройне ополчення хуту, що приймало безпосередню участь у геноциді етнічної меншини тутсі]. Так, виявлено прямий вплив на діяльність людини за допомогою інформаційних технологій - ополченці слухали радіо RTLM і діяли відповідно до інформації, яка транслювалась, а фактично спонукала до виявлення агресії та жорстокості по відношенню до іншої групи населення держави. RTLM активно заохочувало їх до вбивств, невпинно надсилаючи повідомлення про те, що тутсі є ворогами та мають бути знищені раз і назавжди» [99]. За дії, що призвели до масової загибелі людей притягнено до відповідальності директора радіостанції Ф. Нахімана та ведучого Руджу: перший отримав довічний строк ув'язнення, а другий – 12 років позбавлення волі.

Однак, питання стратегії і моделі національної безпеки в інформаційній сфері має полягати у виробленні механізму превентивного визначення дій, що негативно впливають на людей в інформаційній сфері. Необхідним видається аналіз інформаційної війни України та РФ і ролі ЗМІ в ньому обох держав шляхом оцінки наслідків пропаганди, що ними поширюється. Зокрема, аналіз поширення повідомлень за допомогою телебачення, радіо та

друкованих засобів масової інформації. Ефективність пропаганди зростає при підтримці з боку органів державної влади відповідних інформаційних ресурсів [100]. У цій ситуації ЗМІ РФ, що активно транслювали повідомлення та новини на території підконтрольній терористам спричинили хвилю насильства завдяки кумулятивному ефекту (spillover effect – насильство породжує ще більше насильства) серед самого населення включаючи соціальні зв'язки. Кумулятивний ефект стосувався насамперед вербування терористів як серед мешканців РФ, так і населення Донецької та Луганської областей України, що засвідчують інтерв'ю із взятими у полон терористами [101]. Цей ефект менш помітний серед комунікацій звичайних громадян, коли мова йде про невеликий відсоток індивідуального насильства. ЗМІ РФ створили міф, що «Росія як дружня держава рятує українців, що проживають на території Донецької та Луганської областей від нібито «тиску» на російськомовне населення цих територій. Дані технології пропаганди активно використовуються як колись у Руанді РФ для поширення власного бачення ситуації, просування ідеї створення ЛНР та ДНР і інших планів сепаратистів. Основне завдання, що виконують російські ЗМІ своїми діями на Сході України – формування негативного іміджу української влади, військовослужбовців. Інформаційні атаки РФ включають: трансляцію репортажів про «звірства українських військовослужбовців».

Так, російський телеканал ОРТ показав сюжет про те, що українські бійці отримали наказ вбивати мирне населення, а в нагороду за дані дії повинні отримати «клаптик землі та два раба» [102]. Схожим за змістом матеріалом ідею створення негативного образу українських військових займався телеканал РЕН-ТВ, що поширював відео та повідомлення про «вбивства мирного населення українськими військовими у селищах Саурівка і Степанівка Донецької області, де нібито бійці української Нацгвардії вбивали всіх чоловіків, а жінок ґвалтували [103].

Головні повідомлення, що розповсюджують ЗМІ Російської Федерації, зокрема телеканал «Россия», включають текст про «фашизм в Україні» для маніпулювання людською свідомістю. В інтерв'ю *DW* російський соціолог Лев Гудков запевнив: «За допомогою пропаганди, українські націоналісти загрожують росіянам на Сході України». Більшість кадрів, що транслює російське телебачення включають показ українських військових із зброєю в руках, які нібито із жорстокістю вбивають мирне населення, а сепаратисти представлені виключно як захисники місцевого населення. Так, пропаганда у Росії даних ідей має свої результати: відповідно до результатів російського «Аналітичного центру досліджень Юрія Левади» більше 50% росіян вважають, що вони отримують «корисну і об'єктивну інформацію», а кожен п'ятий житель Росії вважає, що володіє «повною, об'єктивною картиною зображення подій». Відповідно до результатів опитування, проведеного у червні 2015 року Фондом громадської думки (ФОМ) РФ, 90% росіян вважають телебачення основним джерелом інформації. Таким прикладом маніпулювання фактами у ЗМІ є представлення українського режисера О.Г. Сенцова у якості терориста, якого звинуватили у підпалі офісу проросійської партії в Криму, і в плануванні підірвати пам'ятник Леніну у м. Сімферополь. Заперечення щодо фальсифікації даної справи висунули ряд міжнародних правозахисних організацій, вважаючи його політв’язнем, однак жоден російський телеканал, включаючи «Росію» не транслював даних заперечень і самого кінорежисера, однак показано сюжет із зображенням його як терориста. Так, керівник німецького відділення організації «Репортери без кордонів» Крістіан Мір наголошує на розповсюдженні російськими ЗМІ недостовірної інформації. Наприклад, інтерв'ю з людиною на ім'я Андрій Петков в квітні 2014 року три російські мовники показали із переказом різних історій: на телеканалі «НТВ» дану особу зображено німецьким шпигуном, якого поранили українські екстремісти, на телеканалі «Росія 1» він був українським громадянином, якого атакували українські неонацисти

під час мирної демонстрації проти українського уряду, а у доповіді офіційного представника російського уряду його представлено хірургом, який допомагав пораненим і підстрелений фашистами під час надання медичної допомоги. І прикладів розповсюдження неправдивої інформації російськими мовниками існує багато [105].

Російські мовники за допомогою пропаганди активно проводять інформаційну війну, змішуючи правду і недостовірну інформацію, впливаючи на формування думки населення», - наголошує колишній кореспондент Росії для німецької організації громадського телерадіомовлення ARD Інна Рак, «це стосується і розповсюдження інформації щодо збиття літака МН-17 Малазійських авіаліній на сході України у липні 2014 року». Російські ЗМІ намагались розповсюдити інформацію щодо «побиття пасажирів даного літака після приземлення українськими військовими і їх пряму відповідальність за збиття літака ракетами».

Російські медіа відтворюють відеосюжети про українських військових чи владу у відредагованому вигляді, з відривом від контексту, що напряму створює потенційну загрозу інформаційній безпеці України загалом та національній безпеці зокрема. «Перший канал» РФ у власному випуску новин від 14.11.2014 р. повідомив про те, що Президент України Петро Порошенко збирається економічно тиснути на Донбас, а дітей, що проживають на цій території примусити сидіти в підвалах. У повній версії відеовиступу Президент України говорить лише про те, що так як Донбас «відрізаний» від України озброєними бойовиками, страждають місцеві жителі, які змушені сидіти без пенсій та у підвалах [106]. Ще одним дієвим засобом пропаганди, що використовується в інформаційній війні проти безпеки і цілісності України є використання підроблених фотографій, які демонструють наслідки «звірств», що відбуваються в Україні і

розповсюджуються у соціальних мережах як одному із найефективніших засобів сучасної комунікації людей.

На одній із фотографій у соцмережі «Одноклассники» зображено собак, які обгризають схожі на кістки людини та представлено як актуальне фото зі східної України із підписом: «Собаки доїдають труп українського бійця. ВСУ не забирає українських загиблих, а місцеві жителі відмовляються ховати тих, хто прийшов на їх землю поневолювати і вбивати». Натомість жодного відношення дане фото із подіями на сході України не має [107].

Пропаганді і маніпулятивним технологіям з боку РФ сприяло інформаційне середовище сходу України, в якому відбувався вплив на населення: адже російські телеканали виступали головним джерелом політичних новин для 78 % жителів сходу та півдня України (відповідно до опитування, проведеного фондом Демократичних ініціатив іменем Ілька Кучеріва з 8 по 18 лютого 2014 року) [108]. Ситуацію не змінило і тимчасове призупинення 25 березня 2014 року за рішенням суду (за позовом Національної ради з питань телебачення і радіомовлення) ретрансляції на території України російських каналів «Первый канал. Всемирная сеть», «РТР-Планета», «Россия-24», «НТВ Мир». Більшість місцевих провайдерів не припиняли трансляцію російських телеканалів, у Донецьку і Донецькій області в радіусі до 70 км, що дивиться більше 37 % населення області і мовлення ведуть виключно російські телеканали. [109].

У Луганській області російські телеканали транслюють з об'єктів в Луганську та Ровеньках, які контролює ЛНР (охоплюють близько 56 % населення області) [110]. Що стосується радіомовлення, то в Донецькій області російські радіостанції транслюються тільки з радіорелейних станцій (РРС) Донецька з територією покриття міста і населених пунктів в радіусі до 50 км [111]. За результатами соціологічних досліджень: – близько 17 % населення Луганської та Донецької області підтримують під впливом

телебачення та радіо ідеї відокремлення регіону від України і створення незалежної держави (опитування проведено станом на квітень 2014 р.) [112].

Проаналізовані факти свідчать про прямий вплив пропаганди на формування думки населення і створення потенційної загрози національній безпеці держави та її територіальній цілісності. Задля перешкоджання російській пропаганді і розробляється національна концепція безпеки України в інформаційній сфері, а також створено Міністерство інформаційної політики України. Так, за результатами соціологічного опитування наслідками впливу російської пропаганди серед населення територій Донецької та Луганської областей стало відчуття страху перед радикально налаштованими жителями західної України – «бандерівцями» (загрозу вбачають 60 % опитаних), страху перед українською владою (47 %), страху перед втручанням європейських та американських політиків (38 %), менша частина відчуває страх перед громадянами Росії, які беруть участь в організації проросійських мітингів (23 %) і від російських політиків та військових (21 %) [113].

Кумулятивний ефект пропаганди поєднується із безпосереднім постійним тиском на аудиторію та ефектом, що здійснює пропаганда на її реципієнта. Зацікавленість у пропаганді доповнює спостереження журналіста Бен Юда (Ben Judah): «В. Путін стверджує, що він не користується Інтернетом, натомість щоденно отримує матеріали з питань політики Кремля, внутрішнім справам в Росії та закордонним справам від трьох основних спецслужб [114].

Таким чином, окрім обов'язково врахування критеріїв, наведених в табличці, представленій в попередньому підрозділі, модель інформаційної безпеки України має враховувати усі проаналізовані аспекти пропаганди, що використовується іншою державою (у даному випадку – РФ, фактично, в інтересах зовнішнього агресора) для превентивного ефективного використання у будь-яких сферах і можливих конфліктах задля забезпечення національної безпеки держави. Потрібен чіткий механізм перешкоджання

поширення впливу пропаганди на населення, комплексне дослідження, що використовуватиметься в українській практиці. Автор дослідження виявив пряму залежність між поширенням повідомлень із недостовірною інформацією і формуванням ставлення населення до відповідного питання. Серед ключових напрямків, за якими діяли ЗМІ РФ слід відмітити: переконування населення, що вони створюють незалежну державу, а на проросійськи налаштоване населення здійснюють тиск українські військові; повідомлення, що уряд не каратиме за участь у лавах терористів і за вбивства, що вони вчиняють; повідомлень з погрозами до жителів Донецької та Луганської областей; приниження та образи на адресу українських військових (порівнюючи їх з фашистами). Ефективність діяльності російських ЗМІ обумовлена їх більшою кількістю і сприйняттям на цій території. Тому жителі цих територій сприймали всю інформацію, поширену російськими телеканалами як достовірну та актуальну для прийняття рішень та формування позиції.

Згідно теорії про роль соціальних взаємодій, хвилю масової жорстокості спричинив і кумулятивний ефект (spillover effect), наслідком якого стала просторова дифузія насильства, що відбувається завдяки соціальним зв'язкам. Маніпулятивні механізми, що використовуються у військових конфліктах, завжди мають схожі риси і включають описані вище аспекти пропаганди: систематичні недостовірні телевізійні сюжети про «карателів київської фашистської хунти», репортажі про дії української влади з відривом від контексту, розповсюдження підроблених фотографій у соціальних мережах, які нібито демонструють наслідки жорстокого поводження українських військових на сході України. Ефективність такого інформаційного впливу перш за все спостерігається завдяки переважанню російських джерел інформації в східних регіонах України, адже російські телеканали стали джерелом політичних новин для 78 % мешканців. Використання даних пропагандистських технологій порушує положення

Європейської конвенції про транскордонне телебачення (Ст. 7 – «програми в цілому, їх представлення та зміст повинні забезпечувати повагу до людської гідності та основних прав інших людей… Зокрема, вони не повинні надмірно виділяти насильство і сприяти расовій ненависті [115]. Телемовник повинен забезпечувати, щоб в новинах факти і події подавались справедливо та сприяли вільному формування думок»).

Для перешкоджання впливу пропаганди потрібно: 1) визначити механізм підтвердження факту здійснення пропаганди проти України для проведення судових експертиз та порушення судових справ; 2) вироблення механізму спростування недостовірної інформації - контрпропаганди, 3) покращення знань населення у сфері інформаційних технологій і власної інформаційної безпеки, 4) постійне інформування населення шляхом медіа-джерела об'єктивної інформації про ситуацію в державі. Таким чином зображено вплив ЗМІ на поведінку шляхом впливу на переконання чи уподобання [115].

В моделях, що будуються на переконаннях (belief-based models), одержувачі інформації виступають як раціональні агенти, які відповідно до теореми Байєса сприймають інформацію як достовірну та актуальну для формування власної позиції та прийняття рішень, а також містить дані про очікувані витрати або вигоди альтернативних рішень, що підтверджено на прикладі використання радіо при геноциді у Руанді [116]. Модель, в основі якої лежать преференції (preference-based models) припускає, що неінформативний емоційно забарвлений зміст впливає на поведінку, навіть якщо агенти не є цілком раціональними. Маніпулювання настроями та провокування відчуття ненависті за допомогою таких методів, що виявляється у використанні ярликів «фашисти», «хунта», відіграє як самостійну так і додаткову роль в процесі формування внутрішньої мотивації до насильства [100]. Використання даних технологій призвело до окупації частини території України і поширення насильства на них [117].

Інформаційні атаки у сучасному світі є більш ефективними, ніж військові дії. Та, на жаль, інформаційна безпека України залишається найбільш вразливою ланкою національної безпеки України [118].

Постійний інформаційно-психологічний тиск РФ на соціальні групи будь-якої держави є специфічною рисою інформаційної війни РФ і телебачення один із найпотужніших каналів впливу. З метою посилення можливостей впливу ЗМІ РФ на ефективність сприйняття інформації широкими верствами населення різних країн, активно використовують інформаційно-комунікативні аналітичні центри. Впродовж 2014 р., інформагенція «РИА-Новости», інформвидання Lenta.ru, RT, та ін. неодноразово замовляли дослідження в Аналітичного центру Brand Analytics, створеного на базі однієї з провідних ІТ-компаній РФ, також активно працюють із пропагандою російськомовний сайт Russia Today (більше ніж 6 млн посилань) та РИА Новости (5,6 млн посилань) та новий мультимедійний Інтернет-проект Sputnik, новинні ресурси LifeNews, Вести.ru, ТАСС, Sports.ru, «Эхо Москвы» та сайт газети «Комсомольская правда» [119]. Поява агресивного пропагандистського російського інформаційного продукту у медійному просторі США та країн ЄС останнім часом стала викликати занепокоєння в контексті посилення не прихованого інформаційного тиску на населення, що пов’язано медіа експертами з активізацією роботи каналу RT і розширенням інформаційних ресурсів РФ. Журналістом видання Business Insider проведено експеримент над своєю свідомістю: тиждень переглядаючи новини телеканалу RT він спостерігав за зміною власної позиції до конфлікту на сході України. Як результат - вплив на свідомість глядача, створення викривленого погляду на події та виключення будь-яких альтернативних тлумачень подій.

У США контрпропагандою займається Рада керуючих з питань мовлення ЗМІ США (BBG), яку очолює Е. Лак [120]. Її основною функцією є підвищення якості роботи американських ЗМІ. Наявність потужної

пропаганди РФ підтверджено у заяві головнокомандувача об'єднаними силами НАТО в Європі Ф. Брідлава, зроблена 22 березня 2015 р. в Брюсселі стосовно того, що Захід повинен вжити більше зусиль для протидії російській пропаганді щодо конфлікту в Україні: «Необхідно негайно реагувати на дезінформацію, поширювану Росією в соцмережах… Потрібно розкривати факти дезінформації й демонструвати їх» [120]. Також РФ використовує для розповсюдження необхідного контенту невеликі європейські ЗМІ місцевого значення [121].

«За словами Т. Снайдера, відомого американського історика, професора Єльського університету: «мета російської пропаганди в тому, щоб показати, що правди, по суті, не існує» [122]. Російські спецслужби вже тривалий час використовують наявні інформаційні ресурси ЗМІ РФ для проведення інформаційно-психологічних спецоперацій з метою маніпулювання суспільною свідомістю як громадян сусідніх країн, так і громадян країн євроатлантичного простору. [http://www.novayagazeta.ru/politics/67000.html]. Ефективною маніпулятивною технологією управління масовою свідомістю громадян різних країн стала створена у РФ «Агенція Інтернет-троллів-дописувачів», які розповсюджують потрібну інформацію у соціальних мережах, комунікуючи на блогах, коментуючи статті та на форумах [123].

Із врахуванням вищевикладеного, можна з упевненістю стверджувати, що сьогодні проти України ведеться «гібридна війна» з потужною інформаційною складовою, як на території нашої держави так і в світовому інформаційному просторі.

• У сфері державної безпеки відбувається посягання на суверенітет та територіальну цілісність України;

• У внутрішньополітичній сфері викривляється та неправдиво подається інформація про критичний стан національних меншин у нашій державі, порушуються питання другої державної мови;

• У зовнішньополітичній сфері поширюється недостовірна, упереджена та неповна інформація про Україну, формується негативна світова громадська думка з метою просування власних інтересів;

• У воєнній сфері Україна дискредитується у якості надійного та передбачуваного партнера у питаннях продажу озброєння третім країнам з порушенням норм міжнародного права;

• У економічній сфері;

• У соціально-гуманітарній сфері;

• У науково-технічній сфері;

• У екологічній сфері.

Ключовими елементами «гібридної війни» РФ проти України є:

- Окупація українських територій, розхитування українського суверенітету
- Енергетичний тиск;
- Торгівельно-економічна війна;
- Фінансування терористичних, сепаратистських рухів;
- Пропаганда, маніпуляція суспільною думкою (підміна понять).

Головними тезами російської інформаційної пропаганди є: Крим з історичної, культурної та ментальної точки зору ніколи не був українським, його повернення в РФ є природним явищем; РФ діє виключно з метою захисту російської меншини від радикально налаштованих українських націоналістів; жителі Луганської та Донецької областей самостійно виявляють прагнення увійти до складу РФ, з боку РФ допомога в реалізації даних намірів не надається; Україна розділена на схід і захід, їй потрібна федералізація; в державі триває громадянська війна; загибель мирних людей є спланованою акцією влади України; через «каральну операцію» української влади на сході гинуть мирні люди, тому влада має негайно припинити її без будь-яких умов і сісти за стіл переговорів з власним народом; після державного перевороту в Києві продовжує діяти «хунта» і «нацистський

режим»; хоч діючий Президент України і легітимний, але прийшов до влади не зовсім правовими методами (посилання на власну статтю).

Інструменти інформаційно-психологічного впливу, що використовує РФ: вибіркові повідомлення для різних цільових аудиторій (для власної держави», для українського суспільства, західноєвропейського та американського суспільства) 2) викривлення фактів; 3) публікація та тиражування недостовірних фото та відеосюжетів; зображення, зроблені в інших військових умовах 3) підвищення військової могутності Росії; 4) активне використання повідомлення, що «розпад СРСР – геополітична катастрофа XX ст.» (застосовувалась у війні з Грузією у 2008 р.); 5) героїзація російських військових; 6) використання тези про «фашизоване» українське суспільство, 7) використання образу дитини, що плаче впливає на будь-яку аудиторію (російські ЗМІ активно акцентують увагу на тому, що на Донбасі гинуть діти). Необхідно констатувати, що реакція українських ЗМІ на інформаційно-психологічну агресію РФ відбувається із запізненням та не відповідає реальній загрозі.

Пропаганда РФ створює хибне розуміння війни в Україні громадськістю за умови наявності невеликої кількості контенту з цих питань українських ЗМІ. У більшості держав світу питанням іномовлення та формування контенту здійснює міністерство закордонних справ, а у межах власної держави наявні потужні інформаційні ресурси, що висвітлюють достовірну інформацію. Щоб запобігти у майбутньому збільшенню агресивного інформаційно-психологічного впливу на громадян необхідно враховувати, що існує тенденція до зростання ролі соціальних мереж як засобу формування думки споживачів інформації, що може активно використовуватись спецслужбами РФ для подальшої дестабілізації ситуації на сході України. Необхідно активізувати роботу з координації співпраці ЗМІ України та громадських ініціатив з метою об’єктивного та своєчасного

реагування на інформаційну агресію РФ, підвищити роль державних каналів та іномовлення.

Протидія інформаційній агресії та цілеспрямованим кампаніям у іноземних ЗМІ проти України є одним з першочергових елементів гарантування національної безпеки України у зовнішньому вимірі. Інформаційні війни стали поширеним інструментом здобування політико-економічних інтересів держав, котрі прагнуть посилити свій вплив на формування громадської думки в Україні з метою її подальшого використання для реалізації власних зовнішньополітичних стратегій.

Протидія інформаційній агресії та цілеспрямованим кампаніям у ЗМІ проти України є одним з першочергових елементів гарантування національної безпеки України.

Таким чином, для забезпечення інформаційної безпеки як складової національної безпеки України автором пропонується здійснити наступні дії:

1. визначити державну політику та створити необхідну інфраструктуру в інформаційній сфері;

2. швидшими темпами забезпечити входження України у світовий інформаційний простір;

3. попереджати інформаційні атаки з боку інших держав за допомогою діяльності відповідних органів державної влади і витік інформації, що становить державну таємницю;

4. впровадження новітніх технологій захисту інформаційного простору України;

5. підвищити рівень співпраці органів державної влади з моніторингу, виявлення, оцінки і створення прогнозів загроз інформаційній безпеці, запобігання даним загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;

6. вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів,

протидії кібертероризму, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

7. створення, забезпечення діяльності тампостійне покращення державної системи конфіденційного зв'язку як сучасної системи забезпечення захисту інформації.

Автором пропонується вдосконалити національний план дій по розвитку інформаційної сфери наступним чином(пропонується універсальний план дій):

1) розробити національну електронну стратегію;

2) створити інформаційну та комунікаційну інфраструктуру (забезпечення усіх груп населення включаючи людей з особливими потребами та похилого віку до інформаційних технологій

3) забезпечити доступ до інформації та знань

4) підвищення грамотності у сфері інформаційно-комунікаційних технологій

5) зміцнення довіри населення держави до інформації (співробітництво між державами в рамках ООН, підвищення обізнаності користувачів з механізмами боротьби з кіберзлочинністю).

Так як тенденція у світі спостерігається до розширення інформаційних технологій і їх використання в усіх сферах(економіці, охороні здоров'я, освіті) актуальним постає питання превентивних дій по захисту усієї інформації від кібератак. Дані системи до їх впровадження наприклад електронного врядування мають бути надійно захищені.

6) застосування електронного державного управління, поширення мережевої освіти та системи охорони здоров'я онлайн

7) збереження культурного і мовного розмаїття шляхом створення різноманітного інформаційного контенту, перекладу в цифрову форму спадщини в галузі освіти, науки й культури, розробку й поширення програмного забезпечення регіональними мовами.

8) боротьба із контентом у ЗМІ, агресивною пропагандою.

У довгостроковій перспективі відродження в Україні також відкриває додаткові можливості для створення позитивного іміджу України за кордоном та руйнації історичних стереотипів про нашу країну, створених РФ. З метою розширення співпраці України з країнами ЄС в гуманітарній сфері можна розглянути можливість збільшення просвітницьких проектів схожих на діяльність Британської ради чи італійської спілки Данте Аліґ'єрі в Україні. Потрібно створити розгалужену мережу для розповсюдження українського контенту за межі Україні відповідно іноземними мовами для чого мають активно співпрацювати РНБО, Президент України, МЗС, Національна рада з питань телебачення та радіомовлення [118].

Висновки до розділу 3.

Інформаційна безпека - невід'ємний та один із ключових елементів національної безпеки держави. У свою чергу, національна безпека є похідною від виробничого й економічного, соціально-політичного та культурного розвитку країни, її ролі й місця в системі міжнародних відносин.

З розвитком технологій інформаційна безпека стала ще більш складною і високозабезпечуваною. Кожного дня держави мають удосконалювати концепцію саме інформаційної безпеки, адже інформаційні загрози національним інтересам значно динамічніше, ніж економічні чи політичні, виникають нові технологій, механізми засоби. Держава стає перед викликом: кожного дня шукати нові шляхи та засоби протидії інформаційним загрозам.

Однак, потрібно враховувати, що національна безпека тісно пов'язана з міжнародною. Інформаційна безпека і її модель має вирішуватись на державному рівні, вищими органами державної влади та відповідати національним інтересам життєвої ваги.

Питання національної інформаційної безпеки найбільш гостро постало саме перед країнами, які тільки вибороли незалежність, суверенітет, стали економічно самостійними. Концепції інформаційної безпеки розроблені і діють у більшості держав світу і Україна не є винятком. Майже усі такі концепції зумовлені двома обставинами: перша - захист національного інформаційного простору та його безпека; друга - інтеграція національних інформаційних просторів у світовий. Україна при формуванні національного інформаційного простору має враховувати дані обставини, розвиваючи його та захищаючи.

Базовими елементами національної інформаційної безпеки виступають: національні інтереси – загроза – захист. Метою інформаційної безпеки держави є захист суспільних відносин.

Для вироблення необхідної моделі інформаційної безпеки необхідно визначити загрози інформаційній безпеці, що проаналізовано у попередньому розділі дослідження. На разі вдалось виявити відсутність єдності у поглядах, що стосуються класифікації відповідних загроз як на нормативно-правовому, так і на науковому рівнях. Доктрина інформаційної безпеки України визначає основні реальні та потенційні загрози інформаційній безпеці України класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері, внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, в екологічній сфері.

Як свідчать наукові дослідження, проблемами системи забезпечення інформаційної безпеки України виступають: неефективність менеджменту (її управління), відсутність систематичності і постійного вдосконалення, відсутність координації між різними органами державної влади, що її забезпечують. Згідно зі статтею 17 Конституції України забезпечення інформаційної безпеки – справа усього українського народу.

Важливо зазначити, що сфері інформаційних технологій притаманна зміна термінології, методів та способів передачі, одержання інформації, що призводить до проблеми коли одне поняття описується різними термінами. Наприклад, під поняттям «інформаційні війни» фахівці технічних галузей знань розуміють порушення електронної інфраструктури суспільства (у розвинених країнах – мережі державних та фінансових установ, таких як управління транспортом, військові системи, що піддаються атакам кібертерористів). У разі, коли здійснення терористичного акту буде поєднано з атакою на інформаційну систему рятувальних служб, медичних закладів чи правоохоронних органів, збитки від даних дій будуть значними. Дані загрози призвели до появи у системі національної безпеки спеціальних силових підрозділів, що володіють інформаційною зброєю та необхідними методами захисту.

Протидія інформаційній агресії та цілеспрямованим кампаніям у іноземних ЗМІ проти України є одним з першочергових елементів гарантування національної безпеки України у зовнішньому вимірі. Інформаційні війни стали поширеним інструментом здобування політико-економічних інтересів держав, котрі прагнуть посилити свій вплив на формування громадської думки в Україні з метою її подальшого використання для реалізації власних зовнішньополітичних стратегій.

Україна є об’єктом потужної спланованої інформаційної агресії деяких сусідніх з нею держав (на сьогоднішній день в першу чергу Росії), а тому має враховувати усі вище написані аспекти при розробці нової більш ефективної концепції інформаційної безпеки, яка має врахувати сучасні тенденції розвитку соціальних мереж, механізмів ведення інформаційних воєн та розвиток інформаційних технологій.

Варто на загальнодержавному рівні надавати ресурсне та організаційно-технічне сприяння телерадіокомпаніям та друкованим ЗМІ України, котрі

своєю діяльністю сприяють поширенню позитивної інформації про нашу державу у європейському та світовому інформаційному просторі.

Таким чином, діяльність держави та ЗМІ мають спрямовуватись на розширення присутності «української тематики» у міжнародному інформаційному просторі, що стало б протидією деструктивним кампаніям у міжнародному інформаційному середовищі, спрямованим проти України. Цей крок є також позитивним у напряму зміцнення інформаційного сегменту національної безпеки нашої держави, котрий наразі перебуває під постійним агресивним впливом певних держав, де інформація про Україну подається упереджено, не об'єктивно та носить переважно дискредитаційний характер. Відсутність належної симетричної реакції з боку нашої держави на подібні випади провокує, у свою чергу, посилення ступеню тиску на українське суспільство, особливо з огляду на те, що телерадіокомпанії деяких прикордонних держав мають право поширювати своє мовлення на українську територію.

На разі, поставши перед проблемою охорони свого суверенітету на тільки в територіальному аспекті, а й в інформаційному, Україна має рішуче та ефективно діяти у відповідній сфері. Використовуючи зарубіжний досвід та його аналіз через призму викликів та загроз, які відчуває на собі Україна, пропонується діяти наступним чином: визначити державну політику та створити необхідну інфраструктуру в інформаційній сфері; швидшими темпами забезпечити входження України у світовий інформаційний простір; попереджати інформаційні атаки з боку інших держав за допомогою діяльності відповідних органів державної влади і витік інформації, що становить державну таємницю; впровадження новітніх технологій захисту інформаційного простору України; підвищити рівень координації державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;

вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії кібертероризму, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвиток Національної системи конфіденційного зв'язку як сучасної системи захисту інформації.

Автором пропонується вдосконалити національний план дій по розвитку інформаційної сфери.

Працівники засобів масової інформації під «інформаційними війнами» розуміють нав'язування певної суспільної думки за допомогою засобів масової інформації, у тому числі через електронні видання та соціальні мережі.

Якщо на побутовому рівні різне тлумачення визначень розуміють і аналізують виходячи з контексту повідомлення, то у правозастосуванні понятійна невизначеність призводить до нівелювання правової основи.

Таким чином інформаційна безпека кожної держави сприятиме забезпеченню глобальної безпеки. Україна має забезпечити власну інформаційну безпеку і зробити свій внесок в сталий розвиток суспільства, захистити власних громадян від кіберзлочинності. Саме кіберпростір – тема для дискусій в усіх міжнародних організаціях, адже єдиних уніфікованих правил його регулювання не існує, кожна держава розробляє власний національний план інформаційної безпеки, враховуючи особливості. Недарма усім відомий вислів «Хто володіє інформацією – той володіє світом» у сучасних реаліях можна інтерпретувати «хто розповсюджує та створює інформацію – той володіє світом».

ВИСНОВКИ

На сьогоднішній день інформація є чи не найважливішим ресурсом, зо забезпечує життєдіяльність держав та світового співтовариства. Це навіть більше, ніж спосіб володіти світом. Завдяки прогресивному розвитку інформаційних і комунікаційних технологій створюються умови для ефективного використання знань та інформації для вирішенні найважливіших завдань управління суспільством в межах однієї держави та по всьому світу.

Успішний розвиток світової спільноти на чолі з суверенними державами та міжнародними організаціями, які стали на шлях постіндустріальної цивілізації розвитку інформаційного суспільства, залежить від інформаційного впливу.

Інформаційний чинник в останні роки спричинив революційні зміни. Зараз увесь світ включений в єдину інформаційну систему, причому вона працює фактично в режимі реального часу.

На даний час найважливішою формою соціальної взаємодії стає інформаційна взаємодія різних груп у суспільстві, від особливостей, характеру та спрямованості якої залежить стан справ у державах і навіть їх взаємовідносини.

У соціальному середовищі постійно створюються, затверджуються і трансформуються високі технології, які проектуються на структури соціальних цінностей. Фактично такі технології формують стратегію розвитку цивілізації з її культурною та духовною сферами.

Людство перейшло в епоху розвитку інформаційного суспільства і отримало таким чином могутній інструмент для об'єднання зусиль з метою одержання нових знань, спрямованих на рішення своїх глобальних проблем, економічного зростання і підвищення життєвого рівня населення.

Поняття інформації нерозривно пов'язане з феноменом комунікації. Комунікація сприяє розвитку людини і є прямо-пропорційною рівню її соціалізації, адже комунікація розвивалась і вдосконалювалась так само як розвивалась і вдосконалювалась людина.

Відповідно виділяться масова комунікація як систематичне та одночасне поширення однотипних повідомлень у великих аудиторіях з метою інформування та здійснення ідеологічного, політичного, економічного, психологічного, організаційного впливу на думки, оцінки і поведінку людей та як вид соціально-культурної діяльності, що відбувається у формі взаємного об'єднання інтелектуальної і емоційної дії, спрямованої на духовний, професійний зв'язок групи людей.

Особливого значення на сьогодні набуває здатність ЗМК управляти розумами сотні мільйонів людей внаслідок глобального їх поширення. Усвідомлюючи можливості засобів масової комунікації, відповідно, варто говорити про необхідність та, звичайно, бажання управління таким важливим ресурсом, оскільки завдяки управлінню цим ресурсом здійснюється управління соціальними системами – окремими індивідами та суспільствами в цілому з метою задоволення інтересів суб'єкта, який здійснює таке управління. Найбільш відчутний такий взаємозв'язок у контексті взаємодії ЗМІ та політичних еліт, особливо під час передвиборчих кампаній. Легітимізація владних дій, створення позитивної громадської думки щодо владних структур, підтримка домінуючих ціннісних орієнтирів у суспільстві - саме цього влада чекає від мас-медіа.

Розвиток ЗМІ спричинив зміни в суспільній психології та способи мислення людей. Вплив ЗМІ на громадськість зумовлюється такими функціональними завданнями як донесення інформації про подію та зміна реальності й управління нею, зміна громадської думки. З цією метою використовується на практиці такий спосіб соціального управління як маніпуляція (з метою змусити більшість (або меншість) брати участь (або не

брати участь) в укоріненні певної практики). Вона є одним з основних засобів соціального контролю та базується насамперед на жорсткому використанні інформаційного апарату і апарату формування ідей.

ЗМІ відіграють фактично ключову роль у впливі на громадську думку. Однак, дедалі ширше залучаються й інші засоби масової комунікації (інші платформи), зокрема соціальні мережі, для посилення контролю за інформацією з метою управління громадською думкою. Так, соціальні мережі (в дипломатії навіть набув відповідного поширення термін твітер-дипломатія) – це платформа для спілкування між абсолютними різними індивідуумами, представниками різних груп населення здатна впливати та проектувати певні зміни в цілому суспільстві та навіть державі (актуальний приклад – координація дій активістів як рушія суспільних перетворень в певних країнах через соціальні мережі).

Отже, не викликає сумнівів і твердження, що за допомогою комунікацій і цілеспрямованої систематизованої інформації в суспільстві можливо реалізувати будь-яку ідею - змінити сприйняття навколишнього середовища, загальноприйнятих людських цінностей, і навіть світу в цілому індивідом або навіть суспільством (вікна Овертона та культивація).

Можна з упевненістю говорити, що вразливість до маніпуляції залежить від різних факторів: від соціального статусу до рівня освіченості. Доведено, що суспільство з низьким соціально-економічним устроєм більш вразливе до технологій маніпулювання ніж розвинуте. Безперечно, на ЗМІ покладена «місія» тримати свідомість аудиторії «під контролем» і з цією метою вони виступають «сурогатами зрілих соціальних ідей», які і пропонуються «сірій масі». ЗМІ мають відповідально ставитися до такої влади.

Інформаційний простір на сьогодні виконує такі основні функції: інтегруюча (об’єднання у просторово-комунікативне і соціокультурне середовище різних видів діяльності); комунікативна (створюється особливе середовище транскордонної, інтерактивної і мобільної комунікації різних

суб'єктів, у рамках якої вони здійснюють інформаційний обмін); актуалізуюча (в інформаційному просторі здійснюється актуалізація інтересів різних суб'єктів діяльності шляхом реалізації ними інформаційної політики); геополітична (формуються власні ресурси і змінюється значущість традиційних ресурсів, створюючи нове середовище геополітичних відносин і конкуренції).

Саме за допомогою інформації можуть ефективніше за будь-яку зброю впливати на населення будь-якої держави зовнішні агресори, адже новини проходять складний шлях від факту до сприйняття, причому на цьому шляху інформація може мимовільно чи навмисне бути викривленою для її неправильного сприйняття аудиторією. В такому разі медіа-картина світу може значно відрізнятись. Задля уникнення цього потрібно досліджувати усі види інформації, можливості захисту інформації, що містить державну таємницю, методи боротьби із пропагандою.

Інформаційний простір є більш ефективним у державах, де він відкритий для суспільства, де втілено реалізацію спільних інтересів громадян, суспільства та держави. Ефективний інформаційний простір держави створюється та розвивається виключно на базі якісної державної соціально-комункаційної політики, що спрямовує до побудови інформаційного суспільства.

Однією з характеристик інформаційного простору є його «трансісторичність».

Найбільш поширений та актуальний спосіб використання інформації та формування потрібного інформаційного середовища у соціальнокомунікаційному вимірі є залучення «лідерів думок». Саме вони достатньо сильно впливають на трансформацію думки, особливо у сфері політики. Вони активно користуються матеріалами мас-медіа і мають більше знань із цього предмету, аніж інші громадяни. Таким чином, лідери думок знаходяться на стику масової та міжособистісної комунікації.

Термін «соціальна комунікація» є комплексним і використовується для позначення всіх типів передачі змісту між відправником та одержувачем, з використанням технології і за допомогою агентів, які не можуть бути кількісними, адже це процес і дія одночасно.

Усі держави мають за основну мету – забезпечення національно безпеки і інформаційної безпеки як її складової. Вона досягається саме завдяки контролю та регулюванню інформаційного простору. Чим більш розвинена держава, тим більше уваги вона на сьогодні приділяє забезпеченню власної інформаційної безпеки (держава концентрується забезпечення такої безпеки на нормативно-правовому та на виконавчому рівнях, а також відповідно працює з населенням).

Як відомо, сьогодні відносини між Україною та Росією вкрай складні. Щонайменше, дві країни перебувають у стані інформаційної війни (Росія веде її на території України, яка є слабкою в програмному забезпеченні і не може блокувати шкідливу інформацію. Україна, в свою чергу, не має широкого доступу до ЗМІ, в тому числі і Інтернет, в Росії, тому глобальну інформаційну війну вести не може, а лише відбивається від постійних інфоатак).

Як свідчать наукові дослідження, проблемами системи забезпечення інформаційної безпеки України виступають: неефективність менеджменту (її управління), відсутність систематичності і постійного вдосконалення, відсутність координації між різними органами державної влади, що її забезпечують.

Інформаційна безпека з кожним днем стає більш вагомішою для забезпечення національної безпеки держави. У свою чергу, національна безпека є похідною від виробничого й економічного, соціально-політичного та культурного розвитку країни, її ролі й місця в системі міжнародних відносин.

З розвитком технологій інформаційна безпека стала ще більш складною в контексті її забезпечення, особливо враховуючи у цьому зв'язку відносність поняття «суверенітет держави». Кожного дня держави мають удосконалювати концепцію саме інформаційної безпеки, адже інформаційні загрози національним інтересам розвиваються значно динамічніше, ніж економічні чи політичні; весь виникають нові технологій, які породжують нові небезпеки та виклики.

Однак, потрібно враховувати, що національна безпека тісно пов'язана з міжнародною. Інформаційна безпека і її модель має вирішуватись на державному рівні, вищими органами державної влади та відповідати національним інтересам життєвої ваги.

Питання національної інформаційної безпеки найбільш гостро постало саме перед країнами, які тільки вибороли незалежність, суверенітет, стали економічно самостійними. Концепції інформаційної безпеки розроблені і діють у більшості держав світу і Україна не є винятком. Майже усі такі концепції зумовлені двома обставинами: перша - захист національного інформаційного простору та його безпека; друга - інтеграція національних інформаційних просторів у світовий. Україна при формуванні національного інформаційного простору має враховувати дані обставини, розвиваючи його та захищаючи.

Базовими елементами національної інформаційної безпеки виступають: національні інтереси – загроза – захист. Головною метою інформаційної безпеки держави є захист суспільних відносин.

Україна є об'єктом потужної спланованої інформаційної агресії, а тому має враховувати певні аспекти при розробці нової більш ефективної концепції інформаційної безпеки, яка має врахувати сучасні тенденції розвитку соціальних мереж, механізмів ведення інформаційних воєн та розвиток інформаційних технологій. Варто на загальнодержавному рівні надавати ресурсне та організаційно-технічне сприяння телерадіокомпаніям та

друкованим ЗМІ України, котрі своєю діяльністю сприяють поширенню позитивної інформації про нашу державу у європейському та світовому інформаційному просторі. Видається важливим звернутися до досвіду інших країн для наслідування прикладу регулювання сфери інформаційної безпеки, зокрема, Великобританії, де правоохоронні органи постійно співпрацюють із ІКТ-провайдерами.

Доктрина інформаційної безпеки України визначає основні реальні та потенційні загрози інформаційній безпеці України класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері, внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, в екологічній сфері.

Проблемами системи забезпечення інформаційної безпеки України виступають неефективність управління, відсутність систематичності і постійного вдосконалення, відсутність координації між різними органами державної влади, що її забезпечують.

Працівники засобів масової інформації під «інформаційними війнами» розуміють нав'язування певної суспільної думки за допомогою засобів масової інформації, у тому числі через електронні видання та соціальні мережі.

Якщо на побутовому рівні різне тлумачення визначень розуміють і аналізують виходячи з контексту повідомлення, то у правозастосуванні понятійна невизначеність призводить до нівелювання правової основи.

Протидія інформаційній агресії та цілеспрямованим кампаніям у іноземних ЗМІ проти України є одним з першочергових елементів гарантування національної безпеки України у зовнішньому вимірі. Інформаційні війни стали поширеним інструментом здобування політико-економічних інтересів держав, котрі прагнуть посилити свій вплив на

формування громадської думки в Україні з метою її подальшого використання для реалізації власних зовнішньополітичних стратегій.

З метою ефективного забезпечення інформаційної безпеки Україні варто на загальнодержавному рівні надавати ресурсне та організаційно-технічне сприяння телерадіокомпаніям та друкованим ЗМІ України, котрі своєю діяльністю сприяють поширенню позитивної інформації про нашу державу у європейському та світовому інформаційному просторі.

Таким чином, діяльність держави та ЗМІ мають спрямовуватись на розширення присутності «української тематики» у міжнародному інформаційному просторі, що стало б протидією деструктивним кампаніям у міжнародному інформаційному середовищі, спрямованим проти України.

Цей крок є також позитивним у напряму зміцнення інформаційного сегменту національної безпеки нашої держави, котрий наразі перебуває під постійним агресивним впливом певних держав, де інформація про Україну подається упереджено, не об'єктивно та носить переважно дискредитаційний характер. Відсутність належної симетричної реакції з боку нашої держави на подібні випади провокує, у свою чергу, посилення ступеню тиску на українське суспільство, особливо з огляду на те, що телерадіокомпанії деяких прикордонних держав мають право поширювати своє мовлення на українську територію.

Типовим для усіх країн світу є вироблення механізмів забезпечення інформаційної безпеки держави у соціально-комунікаційному плані такими засобами: забезпеченням балансу інтересів особи, суспільства та держави; системне вироблення концепції держави у сфері національної безпеки і соціокомунаційної сфери загалом «набирає обертів», однак, потребує вироблення окремими державами певних акцентів на цьому напрямків; комплексний підхід – налагодження співпраці не тільки між усіма державними органами, що забезпечують безпеку у державі – наприклад Міністерством закордонних справ, Міністерством інформаційної політики та

Міністерством оборони (які, зокрема, представлені в Україні), активна співпраця із науковими інституціями та науково-дослідними інститутами, але й інтеграція з міжнародними системами безпеки, участь у розробці й послідовна імплементація уніфікованих правила забезпечення інформаційної безпеки на різних міжнародних форумах. Зокрема, забезпечення інформаційної безпеки держави залежить також від ефективності публічної демократії, налагодження зв'язків між державами, покращення співпраці шляхом проведення міжнародних конференції, а так просування позитивного іміджу держави за кордоном, спрямування її представлення в «найкращому світлі», орієнтоване на пересічних громадян, які в перспективі мають бути «іноземними адвокатами» держави.

Протидія інформаційній агресії та цілеспрямованим кампаніям у ЗМІ проти України є одним з першочергових елементів гарантування національної безпеки України.

Таким чином, для забезпечення інформаційної безпеки як складової національної безпеки України автором пропонується здійснити наступні дії:

1. визначити державну політику та створити необхідну інфраструктуру в інформаційній сфері;

2. швидшими темпами забезпечити входження України у світовий інформаційний простір;

3. попереджати інформаційні атаки з боку інших держав за допомогою діяльності відповідних органів державної влади і витік інформації, що становить державну таємницю;

4. впровадження новітніх технологій захисту інформаційного простору України;

5. підвищити рівень координації органів державної влади щодо оцінки і прогнозування загроз інформаційній безпеці держави, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародної співпраці з цих питань;

6. вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії кібертероризму, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

7. розгортання та розвиток Національної системи конфіденційного зв'язку як сучасної системи захисту інформації.

Автором пропонується вдосконалити національний план дій по розвитку інформаційної сфери наступним чином (зокрема, пропонується універсальний план дій):

1) розробити національну електронну стратегію;

2) створити інформаційну та комунікаційну інфраструктуру (забезпечення усіх груп населення включаючи людей з особливими потребами та похилого віку до інформаційних технологій;

3) забезпечити доступ до інформації та знань;

4) підвищення грамотності у сфері інформаційно-комунікаційних технологій;

5) зміцнення довіри населення держави до інформації (співробітництво між державами в рамках ООН, підвищення обізнаності користувачів з механізмами боротьби з кіберзлочинністю).

Так як тенденція у світі спостерігається до розширення інформаційних технологій і їх використання в усіх сферах (економіці, охороні здоров'я, освіті) актуальним постає питання превентивних дій по захисту усієї інформації від кібератак. Дані системи до їх впровадження наприклад електронного врядування мають бути надійно захищені.

6) впровадження електронного державного управління, електронної освіти та електронної системи охорони здоров'я;

7) збереження культурного і мовного розмаїття шляхом створення різноманітного інформаційного контенту, перекладу в цифрову форму

спадщини в галузі освіти, науки й культури, розробку й поширення програмного забезпечення регіональними мовами;

8) боротьба із контентом у ЗМІ, агресивною пропагандою.

Таким чином, інформаційна безпека кожної держави сприятиме забезпеченню глобальної безпеки. Україна має забезпечити власну інформаційну безпеку і зробити свій внесок в сталий розвиток суспільства, захистити власних громадян від кіберзлочинності. Саме кіберпростір – тема для дискусій в усіх міжнародних організаціях, адже єдиних уніфікованих правил його регулювання не існує, кожна держава розробляє власний національний план інформаційної безпеки, враховуючи особливості. Недарма усім відомий вислів «Хто володіє інформацією – той володіє світом» у сучасних реаліях можна інтерпретувати «хто розповсюджує та створює інформацію – той володіє світом».

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Різун В. В. Начерки до методології досліджень соціальних комунікацій [Електронний ресурс] // [Наукова сторінка професора Володимира Різуна] / Інститут журналістики : [сайт]/ - Електронні дані. - Київ, 2011. - Режим доступу: http://journlib.univ.kiev.ua/Nacherky_do_metodologiyi.pdf (01.03.2011). - Назва з екрана.

2. Cohen Julie E. Imagining the Networked Information Society / Configurating the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press: 2011. – 24 p. [Electronic resource]. - Mode of access: http://ssrn.com/abstract=1916233. – Title from the screen.

3. Задорожний А.В., Пазюк А.В. Международное информационное право. Т. 1: Учебное пособие, К.: Феникс, 2013. – Библиотека кафедры международного права.

4. Digital Crossroads: Telecommunications Law and Policy in the Internet Age by Nuechterlein, Jonathan E., 2-nd ed., Massachusetts Inst. Of Technology, 2013. – 506 p.

5. ICT4D: Information and Communication Technology for Development (Cambridge Learning) by Unwin, Tim, Cambridge Uni.Press, 2009. – 386 p.

6. Auerbach, K. 2004. Questions and Answers About The Internet and Internet Governance. [Electronic resource]. — Mode of access: http://www.cavebear.com/rw/igov-qa.html. - Title from the screen.

7. Cohen Julie E. Imagining the Networked Information Society / Configurating the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press: 2011. – 24 p. [Electronic resource]. — Mode of access: http://ssrn.com/abstract=1916233. – Title from the screen.

8. Чічановський А. Інформаційні процеси в структурі світових комунікаційних систем [Текст] : підруч. для студ. вищ. навч. закл. / А.

А.Чічановський, О. Г. Старіш ; Київ. нац. ун-т ім. Т. Шевченка, Ін-т журналістики. - К. : Грамота, 2010. - 567 с.

9. Винер Н. Кибернетика. — М.: Сов. радио, 1968. — С. 31

10. Махлуп Ф. Производство и распространение знаний в США. — М., 1966. — С. 36-37

11. Дубровский Д.И. Идеальное как информация, непосредственно «дання» личности // Управление, информация, интеллект. — М., 1976. — С. 236.

12. Акофф Р., Эмери Ф. О целеустремленных системах. М., 1974. — С. 147.

13. Cherry C. On human communication. — N.-Y., 1957. — P. 154.

14. Різун В. В. До постановки наукової проблеми про особливий статус медіакомунікацій (масового спілкування) в системі соціальних комунікацій [Електронний ресурс] // [Наукова сторінка професора Володимира Різуна] / Інститут журналістики : [сайт] / - Електронні дані. - Київ, 2012- Режим доступу: http://journlib.univ.kiev.ua/Do_postanovky_problemy.pdf (дата звернення до статті). - Назва з екрана

15. Моль А. Теория информации и эстетическое восприятие. — М., 1966. — С. 203.

16. Массовая информация в советском промышленном городе: Опыт комплексного социологического исследования / Б.А.Грушин, Л.Н.Федотова, Е.Я.Таршис и др.; Под общ. ред. Б.А.Грушина, Л.А.Оникова. — М.: Политиздат, 1980. — С. 20

17. Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet / Dutton, William H.; Dopatka, Anna; Law, Ginette; Nash, Victoria. Paris, UNESCO, 2011. – 103 p. [Electronic resourse]. – Mode of access: http://unesdoc.unesco.org/images/0019/001915/191594e.pdf. - Title from the screen.

18. WSIS and the Big Picture, Guy Berger, Mail and Guardian (South Africa) online, January 2, 2004

19. ITU Global Cybersecurity Agenda / High–Level Experts Group (Global Strategic Report). – 2008. – P. 17. [Electronic resource]. — Mode of access: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. - Title from the screen.

20. Tokyo Declaration “Asia-Pacific Renaissance through ICT In the 21st Century”, APT Asia-Pacific Summit on the Information Society, 31 October – 2 November 2000, Tokyo. [Electronic resource]. — Mode of access: http://www.aptsec.org/infosummit//Summit%20WEB/Declaration-SOM-Final1.htm. - Title from the screen.

21. International Encyclopedia of Communication / Ed. by E. Barnouw, G. Gerbner, W. Schramm, T.L. Worth, L. Gross. Univ. of Pensilvania. Oxford Univ. Press. N.Y., Oxford, 1989. Vol. 1-4. http://europa.eu.int/ISPO/docs/promotion/past_events/isad_condusioin.doc

22. Istanbul Declaration, ITU World Telecommunication Development Conference, 18-27 March 2002, Istanbul [Electronic resource]. — Mode of access: http://www.itu.int/ITU-D/conferences/wtdc/2002/declaration.html. - Title from the screen.

23. International conference on e-Government for development, Final Communiqué, Palermo, Italy, 11 April 2002. Istanbul [Electronic resource]. — Mode of access: http://www.palermoconference2002.org/en/home.php. - Title from the screen.

24. Соціологія: Навч. посіб. – К.: Т-во «Знання», 2005. – С. 211-212.

25. Різун В. В. Теорія масової комунікації: Підручник. - К.: Видавничий центр «Просвіта», 2008 - 260 с.

26. Набруско В. Формування громадської думки в умовах легітимації політичної влади (масовокомунікативний вимір) [Текст] : дис... канд. політ.

наук: 23.00.03 / Набруско Віктор Іванович ; Київський національний ун-т ім. Тараса Шевченка. Інститут журналістики. - К., 2006. - 192 арк.: рис. - арк. 172-180.

27. Брайант Дж., С Томпсон. Основы воздействия СМИ / Дж. Брайант, С. Томпсон. - М.: Издательский дом "Вильямс". - 2004. — 432 с.

28. Городяненко В.Г. Соціологія. Підручник для студентів вищих навчальних закладів / В. Городяненко. - Київ: Видавничий центр "Академія". – 2002. - 560 с.

29. Почепцов Г. Теория коммуникации [Электронный ресурс] / Библиотека «Полка букиниста». – Режим доступа: http://business.polbu.ru/pochepcov_communications/ch04_ii.html. - Название с экрана.

30. Каландаров В. Управление общественным сознанием. Роль коммуникативных процессов [Электронный ресурс] / В. Каландаров // Koob. – Режим доступа: http://www.klex.ru/my. - Название с екрана.

31. Шрайнер Ю. А. Концепции интеллектуальных систем / Ю. А. Шрайнер // Научно-информационный обзор. – М.: Наука, 1988. – 134 с.

32. International Encyclopedia of Communication / Ed. by E. Barnouw, G. Gerbner, W. Schramm, T.L. Worth, L. Gross. Univ. of Pensilvania. Oxford Univ. Press. N.Y., Oxford, 1989. Vol. 1-4.

33. Цикунов І. Кібернетичний аналіз інформаційного простору суспільства / І. Цикунов // Політ. менеджмент — 2005. — № 4. — С. 3-15.

34. Філософія, навч. Пос. Надольний, Андрущенко Бойкос. 336-337

35. Інформаційні системи і технології на підприємствах: підручник / В. Л. Плескач, Т. Г. Затонацька. - К. : Знання, 2011. - 718 с.

36. Нестеряк Ю. Державна підтримка ЗМІ: європейські традиції та українська практика // Вісник Київського національного університету імені Тараса Шевченка. Серія: журналістика. - Вип. 10. - 2002. - с.50-52.-0,3 д.а.

37. Михайлин, І. Л. Основи журналістики [Текст] : підр. / І. Л. Михайлин. – К. : ЦУЛ, 2002. – 284 с.

38. Яковенко, М. Інформаційний простір: філософські аспекти формування поняття [Текст] / М. Яковенко // Вісник Національного університету «Львівська політехніка» (Філософські науки) : зб. наук. праць. – 2011. – № 692. – С. 22-27.

39. Шершньова Н. Національний простір як відкрита система [Електронний ресурс] / Н. Шершньова // Науковий блог. - Режим доступу: http://naub.oa.edu.ua/2012/natsionalnyj-informatsijnyj-prostir-yak-vidkryta-systema/. – Назва з екрану.

40. Різун В. В., Партико З. В. Журналістика: інформування чи вплив? Погляд на явище з позиції теорії комунікації // Вісник. Журналістика / Київ. нац. ун-т ім. Т. Шевченка.- 2002.- Вип. 10.- С. 22-23.

41. Дубас О. Інформаційно-комунікаційний простір: поняття, сутність, структур / О. Дубас. [Електронний ресурс]. - Режим доступу: http://dspace.nbuv.gov.ua/xmlui/bitstream/handle/123456789/26693/22-Dubas.pdf?sequence=1. Назва з екрану.

42. Серёгин А. В. Информационное пространство как феномен культуры: дис. … 24.00.01 кандидата культурологии / Серёгин А. В. – М., 2000.– 135 с .

43. Дмитровський О. МАНІПУЛЯЦІЙНИЙ ВПЛИВ ЗМІ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ [Електронний ресурс] / О. Дмитровський // Теле, радіожурналістика. – Режим доступу: http://journ.lnu.edu.ua/vypusk7/n10/tele-and_radio_journalism-10-13.pdf. - Назва з екрану.

44. Поняття загроз інформаційній безпеці [Електронний ресурс] / Навчальні матеріали онлайн. - Режим доступу: http://pidruchniki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi. - Назва з екрану.

45. Про основи національної безпеки України: Закон України: від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. − 2003. – № 39.

46. Гуцу С. Ф. Правові основи інформаційної діяльності [Електронний ресурс]. – Режим доступу : http://studrada.com.ua. - Назва з екрану.

47. Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки : Закон України : від 9 січня 2007 року № 537-V // Відомості Верховної Ради України. − 2007. –№ 12. – Ст. 102

48. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997.01.01]. – [Електроний ресурс] / Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. – Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38883&cat_id=38836

49. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України: від 29 березня 2006 року № 373 // Офіційний вісник України. – 2006. – № 13

50. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – [Електроний ресурс] / Офіційний сайт Державної служби спеціального звязку та захисту інформації України. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38934&cat_id=38836

51. Петрунько О. Агресивне медіасередовище: якісний і змістовий дискурси [Електроонний ресурс] / О. Петрунько. – Режим доступу: http://elibrary.kubg.edu.ua/364/1/O_V_Petrynko_AMEQaS.pdf. - Назва з екрану.

52. Іванов В. Ф. Соціологія масової комунікації: Навч. посіб. — К.: Київ. ун-т, 2000/

53. Городенко, Леся Михайлівна. Засоби масової комунікації у контексті громадської думки: формування, функціонування, жанрові прийоми [Текст] : дис... канд. філол. наук: 10.01.08 / Городенко Леся Михайлівна ; Київський національний ун-т ім. Тараса Шевченка, Інститут журналістики. - К., 2003. - 208 арк. - арк. 181-203.

54. Засоби масової комунікації у контексті громадської думки: формування, функціонування, жанрові прийоми [Текст] : дис... канд. філол. наук: 10.01.08 / Городенко Леся Михайлівна ; Київський національний ун-т ім. Тараса Шевченка, Інститут журналістики. - К., 2003. - 208 арк. - арк. 181-203.

55. Конецкая В. П. Социология коммуникации: Учебник / В. Конецкая. — М.: Междунар. ун-т бизнеса и управления, 1997.

56. Australian Government security classification system [Electronic resource] /Protective security framework // Australian Government. – Mode of access: https://www.protectivesecurity.gov.au/informationsecurity/Pages/AustralianGovernmentSecurityClassificationSystem.aspx). – Title from the screen.

57. Почепцов Г. Г. Смислові та інформаційні війни / Г. Г. Почепцов // Інформаційне суспільство. - 2013. - Вип. 18. - С. 21-27. - Режим доступу:http://nbuv.gov.ua/UJRN/is_2013_18_6

58. Rogers, Everett M. Diffusion of innovations / Everett M. Rogers--4th ed. – NY: The Free Press. - 1983. – 51 p.

59. Городенко Л. Потреба інформації у суспільстві // Сучасне та майбутнє журналістики в плюралістичному суспільстві: Матеріали науково-практично українсько-швейцарського семінару / За ред. А. Москаленка, М. Герольд, В. Іванова. – К.: Центр вільної преси, 1999. – С. 314-316.)

60. Гуцалюк М. Координація діяльності правоохоронних органів та інформаційна безпека / М. Гуцалюк // Центр исследований проблем компьютерной преступности [Електронний ресурс]. – Режим доступу: http://www.crime-research.org/library/Gucaluk.htm

61. Лукашевич М. П., Туленков М. В. Соціологія. Загальний курс Навчальний посібник. - К.: Каравела , 2006.- 408 с.

62. Почепцов Г.Г. Соціальні комунікації і нові комунікативні технології / Почепцов Г.Г. // Комунікація. – 2010. – № 1. – С. 19–26.

63. Decree on the media of social communications «Inter mirifica» [Електронний ресурс]. – Режим доступу: http://www.vatican.va/archive/hist_councils/ii_vatican_council/documents/vat-ii_decree_19631204_inter-mirifica_en.html. - Title from the screen.

64. Холод О.М. Соціальні комунікації : соціо- та психолінгвістичний аналіз: навч. посіб. / Холод О.М. – Львів : ПАІС, 2011. – С. 35., с. 35

65. Різун В.В. Начерки до методології досліджень соціальних комунікацій /Різун В.В. // Світ соціальних комунікацій. – 2011. – Т. 1. – с. 7, 10.

66. Манойло А. Государственная информационная политика в особых условиях: монография / А. Манойло. — М.: МИФИ, 2003. — 388 с.

67. Чекмишев О. В. Риси неототалітаризму в сучасних ЗМК // Актуальні питання масової комінікації. - 2001. - Вип. 1. - С. 19 - 22.

68. Levi-Faur, David, Regulation and Regulatory Governance, Jerusalem Papers in Regulation and Governance, No.1, 2010 [Electronic resources]. – Mode of access: http://regulation.huji.ac.il/dp.php. - Title from the screen.

69. Макаренко Є. А. Європейські комунікації: Монографія. – К.: Центр вільної преси, 2006. – 536 с.

70. Віленський Г. Л. Інформаційне право та право сфери культури. – К.: Центр соціального розвитку освітянства, 2001. – 322 с.

71. Різун В. В., Партико З. В. Журналістика: інформування чи вплив? Погляд на явище з позиції теорії комунікації // Вісник. Журналістика / Київ. нац. ун-т ім. Т. Шевченка.- 2002.- Вип. 10.- С. 22-23.

72. Арістова, І. В. Еволюційний розвиток поняття "інформаційна сфера" [Текст] / І. В. Арістова // Вісник Національного університету внутрішніх справ. Вип. 31. - 2005. - С. 239-245

73. Пазюк А. Міжнародне інформаційне право: теорія і практика : монографія / Андрій Валерійович Пазюк, Київ. нац. ун-т ім. Т. Шевченка.– Дніпропетровськ : Середняк Т. К., 2015.– 446 с.

74. Lessig L. The Law of the Horse : What Cyberlaw might teach // Harvard Law Review. – 1999. – V. 113. – P. 501 – 549

75. Задорожний А. В., Пазюк А. В. Международное информационное право. Учебное пособие: Том 1 / Киевский нацио- нальный университет шимени Тараса Шевченко, Інститут международных отношений. – К. : ЧП «Фенікс», 2013. – 854 с.

76. Яковенко, М. Інформаційний простір: філософські аспекти формування поняття [Текст] / М. Яковенко // Вісник Національного університету «Львівська політехніка» (Філософські науки) : зб. наук. праць. – 2011. – № 692. – С. 22-27.

77. Paul Schiff Berman. Cyberspace and the State–Action Debate. The Cultural Value of Applying Constitutional Norms to 'Private' Regulation // University of Colorado Law Review. – 2000. – P. 1263 – 1310.

78. Носенко В. Компьютерный терроризм. – Мировая экономика и международные отношения. – 2007. – № 3. – С. 29–36 [Электронный ресурс]. – Режим доступа: http://www.viche.info/journal/2016/. – Название с экрана.

79. GCHQ intercepted foreign politicians' communications at G20 summits / The Guardian [Electronic resource]. – Mode of access: http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits. - Title from the screen.

80. Кормич Б. А. Інформаційна безпека: організаційно-правові основи. — К., 2004; Словник іншомовних слів. — К., 2000.

81. Логінов А. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право. – Національна академія внутрішніх справ України. – Київ, 2005.

82. Кузьменко Б. В. Захист інформації : навч. посіб. Ч. 2 / Б. В. Кузьменко, О. А. Чайковська. – К. : Видавничий відділ КНУКіМ, 2009. – 69

83. Гуцу С. Ф. Правові основи інформаційної діяльності [Електронний ресурс]. – Режим доступу : http://studrada.com.ua. – Назва з екрана.

84. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf. - Назва з екрану.

85. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: автореф. дис. канд. наук з держ. упр. : 25.00.01 / Л. О. Євдоченко. – Л., 2011. – 24 с, с. 8.

86. Libicki M. What Is Information Warfare? / M. Libicki // Questia. - 1995. – Mode of access: https://www.questia.com/library/journal/1G1-129891565/what-is-information-warfare. - Title from the screen.

87. Serena Syme, L.Jean Camp. Code as Governance, The Governance of Code [Electronic resource]. – Mode of access: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=297154http://www.cs.cmu.edu/~burnsm/InfoWarfare.html. - Title from the screen.

88. Офіційний сайт Міністерства інформаційної політики [Електронний ресурс]. = Режим доступу: http://mip.gov.ua/documents/7.html. - Назва з екрану.

89. Запорожець О.Ю. Політика Європейського Союз у в сфері інформаційної безпеки // Актуальні проблеми міжнародних відносин : зб. наук. пр. / Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. – К., 2009. – Вип.87,ч.2. – С.36-45.

90. Criminal Justice Act 1977 [Electronic resource] – Mode of access: http://www.legislation.gov.uk/ukpga/1977/45/pdfs/ukpga_19770045_en.pdf. - Title from the screen.

91. What is Ofcom? [Electronic resource] – Mode of access: http://www.ofcom.org.uk/about/what-is-ofcom/. – Title from the screen.

92. Система захисту інформаційного простору від спеціальних інформаційних операцій. [Електронний ресурс] – Режим доступу: http://old.niss.gov.ua/book/Litv/010_1.htm. - Назва з екрану.

93. Бондар Ю. Зміцнення та захист національного інформаційного простору України: проблеми та шляхи забезпечення / Ю. Бондар // Український науковий журнал «Освіта регіону політологія психологія комунікації» [Електронний ресурс] – Режим доступу: http://social-science.com.ua/article/61. - Назва з екрану.

94. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/454/. – Назва з екрану

95. Аналітичний звіт «Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії» / ГО «Телекритика». – 17.04.2015. – Режим доступу: http://osvita.mediasapiens.ua/monitoring/advocacy_and_influence/analitichniy_zvi

t_protidiya_rosiyskiy_informatsiyniy_agresii_spilni_zusillya_zadlya_zakhistu_demokratii/ю - Назва з екрану.

96. Пропаганда спрямована на розпалювання національної та міжнаціональної ворожнечі: проблеми визначення та протидії". Аналітична записка / Національний інститут стратегічних досліджень [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1756/. – Назва з екрану.

97. В сфере средств массовой информации. Нормативные правовые акты в сфере массовых коммуникаций / Федеральная служба по надзору в сфере святи. [Электронный ресурс]. – Режим доступа: http://35.rkn.gov.ru/law/p1463/. – Название с экрана.

98. Указ Президента Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015. - Назва з екрану.

99. Різун В. В., Трачук Т. А. Нарис з історії та теорії українського журналістикознавства: Монографія / Київ. нац. ун-т ім. Тараса Шевченка. - К., 2005. - 232 с.

100. СБУ опублікувала розмову терористів після захоплення у полон російського офіцера / 24 канал. [Електронний ресурс]. – Режим доступу: http://24tv.ua/sbu_opublikuvala_rozmovu_teroristiv_pislya_zahoplennya_u_polon_rosiyskogo_ofitsera_18_n597639. - Назва з екрану.

101. Украинцы воюют, чтобы получить двух рабов из Донбасса и кусок земли" - репортаж "Первого канала" России / Цензор. Нет. [Електронний ресурс]. – Режим доступу: http://censor.net.ua/video_news/310035/ukraintsy_voyuyut_chtoby_poluchit_dvuh_rabov_iz_donbassa_i_kusok_zemli_reportaj_pervogo_kanala_rossii. - Назва з екрану.

102. «Сауровская резня» Нацгвардией / Stopfake. [Електронний ресурс]. – Режим доступу: http://www.stopfake.org/fejk-saurovskaya-reznya-natsgvardiej. - Назва з еркану.

103. Журналисты на Украине: как обьяснить, что ты не агент / DW. [Электронный ресурс]. – Режим доступа: http://www.dw.com/ru/%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D1%8B-%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D0%B5-%D0%BA%D0%B0%D0%BA-%D0%BE%D0%B1%D1%8A%D1%8F%D1%81%D0%BD%D0%B8%D1%82%D1%8C-%D1%87%D1%82%D0%BE-%D1%82%D1%8B-%D0%BD%D0%B5-%D0%B0%D0%B3%D0%B5%D0%BD%D1%82/a-17654278). – Назва з екрану.

104. Behind Russia's TV propaganda machine / DW [Electronic resource]. – Mode of access: http://www.dw.com/en/behind-russias-tv-propaganda-machine/a-18689297. - Title from the screen.

105. Ложь: Петр Порошенко пообещал, что дети Донбасса будут сидеть в подвалах [Электронный ресурс]. – Режим доступа: http://www.stopfake.org/lozh-petr-poroshenko-poobeshhal-chto-deti-donbassa-budut-sidet-v-podvalah/. – Название с экрана.

106. Фотофейк: собаки доедают труп украинского бойца [Электронный ресурс]. – Режим доступа: http://www.stopfake.org/fotofejk-sobaki-doedayut-trup-ukrainskogo-bojtsa/). – Название с экрана.

107. Телебачення як джерело політичних новин - загальнонаціональне опитування / Фонд Демократичні ініціативи імені Кулька Кучеріва. [Електронний ресурс]. – Режим доступу: http://www.dif.org.ua/ua/polls/2014_polls/telebachennja-jak-dzherelo-politichnih-novin---zagalnonacionalne-opituvannja.htm. - Назва з екрану.

108. Нацсовет по телевидению заявляет о вещании исключительно российских телеканалов в радиусе 70 км от Донецка / Новости Донбасса. [Электронный ресурс]. – Режим доступа: http://novosti.dn.ua/details/235868. - Режим доступа.

109. В Нацсовете сообщили, где в Донецкой и Луганской области можно смотреть украинское ТВ / Новости времени. [Электронный ресурс]. – Режим доступа: http://nvua.net/ukraine/V-Nacsovete-soobshchili-gde-v-Doneckoy-i-Luganskoy-oblasti-mozhno-smotret-ukrainskoe-TV-15579.html. - Режим доступа.

110. Чи властиві українцям настрої сепаратизму - загальнонаціональне опитування / Фонд Демократичні ініціативи імені Кулька Кучеріва. [Електронний ресурс]. – Режим доступу: http://www.dif.org.ua/ua/polls/2014_polls/chi-vlastivi-ukraincjam-nastroi-separatizmu_-.htm. - Назва з екрану.

111. Кіпень В. Травмована свідомість як наслідок і фактор нестабільності (дослідження масових настроїв жителів Донецька. [Електронний ресурс]. – Режим доступу: http://skhid.com.ua/article/download/24557/22158. - Назва з екрану.

112. Мнение: Путин - непризнание реальности / Главное. [Електронний ресурс]. – Режим доступу: http://glavnoe.ua/news/n209168. Назва з екрану.

113. The White House, Office of the Press Secretary, Remarks by the President on Review of Signals Intelligence, 17 January 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

114. Дубов Д. New generation dual-use technologies as innovative determinants of national security and defense [Електронний ресурс]. – Режим доступу: http://www.academia.edu/11668108/New_generation_dual-

use_technologies_as_innovative_determinants_of_national_security_and_defens. - Назва з екрану.

115. «Батьківщина» найбільше «джинсувала» в друкованих виданнях, «Заступ» – в інтернеті // Теле-критика. – 09.10.2014 р. [Електронний ресурс]. – Режим доступу: http://vybory.mediasapiens.ua/2014/10/09/batkivschyna-najbilshe-dzhynsuvala-v-drukovanyh-vydannyah-zastup-v-interneti/

116. Prevention of Terrorism (Temporary Provisions) Act 1989 (repealed) [Електронний ресурс]. – Режим доступу: http://www.legislation.gov.uk/ukpga/1989/4/contents

117. Евросоюз разработает план по борьбе с российской пропагандой / DW. [Электронный ресурс]. – Режим доступу: http://dw.de/p/1EsAA

118. The New UK Model of Press Regulation. – March 2014 LSE Media Policy Project [Електронний ресурс]. – Режим доступу: http://www.lse.ac.uk/media@lse/documents/MPP/LSE-MPP-Policy-Brief-12-The-New-UK.