ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ПЕТРА МОГИЛИ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

КАФЕДРА ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

МАГІСТЕРСЬКА РОБОТА

на тему «**ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ В УКРАЇНІ В УМОВАХ ВІЙСЬКОВОГО СТАНУ»**

Виконав: студент 6 курсу 636-д групи
напряму підготовки
28 Публічне управління та адміністрування
спеціальності
281 Публічне управління та адміністрування
Залюбовський Олександр Григорович

Керівник: доктор політичних наук,
професор, зав. кафедри публічного управління
та адміністрування
Євтушенко Олександр Никифорович

Рецензент: кандидат історичних наук, доцент
Малиновська Наталя Леонідівна

Миколаїв – 2022

ЗМІСТ

ВСТУП

Актуальність дослідження полягає в необхідності покращення та розвитку української інформаційної безпеки після перемоги України проти російських окупантів, і, водночас, під час воєнного стану в умовах активної фази війни. Для реформування деяких елементів було б чудово врахувати досвід європейських держав, зокрема Європейського Союзу, курс на вступ до якого взяла Україна. Український інформаційний простір зазнає регулярно інформаційних впливів. Є регулярний значний негативний вплив в цій сфері з боку Російської Федерації з метою дестабілізації та поширення паніки в українському суспільстві.

Для боротьби проти інформаційно-психологічних операцій країни-спонсора тероризму необхідна взаємодія усіх структур, органів, ЗМІ України, а також самих громадян. Українська інформаційна безпека не є ідеальною у сучасному її вигляді, але завдяки неймовірній щоденній роботі «на усіх фронтах», та допомозі цивілізованого Заходу, Україні успішно виходить вигравати боротьбу за розуми та серця населення не лише нашої країни, а й всього світу. Питання вдосконалення інформаційної безпеки та виправлення помилок постає постійно. Доречно в Україні застосовувати усі новітні методи боротьби проти російської пропаганди, неправдивої інформації, дезінформації, тощо.

Потрібно зазначити, що в Україні науковими аспектами інформаційної безпеки людини в Україні присвячені дослідження таких українських вчених, як Д. Беззубов, І. Боднар, Ю. Горбань, В. Горбулін, О. Довгань, О. Дзьобань, О. Золотар, Р. Калюжний, Є. Кравець, О. Лазоренко, М. Левицька, О. Левченко, В. Ліпкан, Є. Магда, Ю. Максименко, Я. Малик, С. Мельник, О. Морозов, В. Петрик, О. Тихомиров та ін.

Правові аспекти інформаційної безпеки вивчають таки відомі українські вчені, як: В. Гавловський, О. Марценюк, О. Олійник, А. Петрицький, В. Тихий, в. Фурашев, В. Цимбалюк та ін.

Мета роботи полягає в аналізі інформаційної безпеки людини в Україні в умовах військового стану, виділенні її основних особливостей; охарактеризувати роль уряду, ЗМІ, громадянського суспільства у боротьби проти дезінформації.

Завданнями цієї роботи є:

– визначити поняття інформаційної безпеки;

– охарактеризувати систему національної інформаційної безпеки України;

– проаналізувати нормативно-правове регулювання інформаційній безпеки;

– надати класифікацію інформаційних загроз та їх вплив на інформаційну безпеку України;

– розглянути особливості правового забезпечення прав і безпеки окремих категорій осіб ;

– обґрунтувати інформаційну захищеність людини в умовах інформаційних впливів Російської Федерації

– надати рекомендації щодо безпеки для громадянина в інформаційному просторі піл час воєнного стану.

Об'єктом дослідження є державна політика інформаційної безпеки в Україні.

Предметом дослідження є інформаційна безпека людини в Україні в умовах військового стану.

Методологія дослідження. Методологічну основу дипломної роботи складає сукупність наукових підходів. Для виконання розроблених завдань використовувались різні методи в цій роботі: метод аналізу, аналогії, історичний метод, прогнозування, метод синтезу. Наприклад, метод

узагальнення надає можливість простежити за розвитком інформаційної безпеки та утворення сучасної національної системи захищеності. Описово-хронологічний метод допомагає провести паралелі у часовому виміри, що відбувались в країні. Аналіз і синтез допомагають дати характеристику діяльності держави під час воєнного стану.

Метод спостереження допомагає провести аналіз ефективності дій уряду в протидії російській пропаганді, фейкам, та дозволяє проаналізувати помилки, успіхи.

Практичне значення роботи полягає в тому, що Україні необхідно удосконалювати законодавство України, посилювати інформаційну безпеку для всіх категорій населення, та боротися проти дезінформації, фейків та інших видів інформаційних впливів. Цю роботу написано в наукових та навчальних цілях, і безпосередньо адресовано викладачам, студентам, аспірантам гуманітарних факультетів. Матеріали магістерської роботи можуть бути використані при написанні освітньо-кваліфікаційних робіт.

Структура магістерської роботи. Відбиває поставлені перед роботою цілі та завдання. Загальний обсяг її становить 90 сторінок, з них основного тексту – 75 сторінок. Магістерська робота складається зі вступу, 3 розділів, списку використаних джерел, та додатків.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інформаційна безпека: характеристика поняття

Людина в давні часи шукала джерело води, інше плем'я, місця для полювання. Наразі інформаційна діяльність також відбувається в сучасних і відомих нам методах, і вона є нерозривно пов'язана з інформаційною безпекою. З розвитком інформаційного суспільства значення безпеки невпинно зростає.

Феномен інформаційної безпеки розглядається як відношення людини до держави і суспільства, відштовхуючись від потреб, інтересів суб'єктів та об'єктів безпеки. Безпека вочевидь впливає на розвиток суспільних процесів. Цим пояснюється актуальність дослідження інформаційної безпеки як суспільного явища.

Етимологічно термін "security" походить від латинського виразу «sine cura», що означає «без» (sine) і догляду, турботи, занепокоєння, заклопотаності (cura). Подібною є етимологія українського терміну «безпека».

Академік Тихий В.П. пропонує наступний етимологічний аналіз слова «безпека» [90]. Слово створено з прийменника «bez" і основи іменника «peka», пов'язаного з дієсловом «pekti» (українською – «пекти») [18, с. 163]. Прийменник «без» має загальнослов'янський індоєвропейський характер. Його вихідне, початкове значення за джерелами – «поза», «крім» [18, с. 161]. Слова «пека» - від слова «пек», яке запозичене з голландської мови («pek» - смола). У старослов'янській мові – «пькъ», «пькълъ» - пекло; смола. У християнстві грішники киплять у пеклі в смолі, горять у вічному вогні; через

те в народній етимології слово «пекло» пов'язується з дієсловом «пекти». Пекло – найнебезпечніше місце [18, с.328-329]. Є також міф про Пека – слов'янського бога пекла. У давньоукраїнській міфології Пек – бог пекла, а також війни, кровопролить, кривавих бійок, всілякої біди, син Чорнобога і Марі. Згідно з повір'ям він був страхітливий, підступний, кровожерливий, нещадний, але лякливий, надто боявся Чура. «Пекло» - царство Пека, страхітливе підземелля, куди «провалювалися» душі росіян після своєї смерті. Битва Чура з Пеком у підземеллі за уявленням давніх українців призводила до землетрусів. Тільки Чур міг забрати з пекла хороших людей, яких Пек затягнув [56, с. 181–182].

Цікаво, що в сучасній польській мові досі залишилась форма «печа» (piecza) – догляд, опіка, турбота. Власне його однокореневим є польське «bezpieczeństwo» - «безпека». Таким чином, етимологічне походження поняття «безпека» узалежнює його від небезпек, загроз і ризиків.

Нові реалії і соціальні зміни вимагають переглянути зміст безпеки в цілому, так і інформаційної безпеки. Тлумачать це поняття різними способами. Є енциклопедичні, доктринальні, і нормативно-правові визначення. Методологічні підходи, логічні способи, сфери існування суттєво відрізняються. Категорія безпеки неоднозначна і визначається в залежності від наукової області, в якій вона вивчається.

Інформаційне протиборство є природнім станом в умовах конкуренції глобалізованого світу. Необхідно забезпечувати інформаційну і кібернетичну безпеку. Цьому приділяється особлива увагу задля забезпечення тих самих інтересів на рівнях особи, суспільства, держави, міжнародного правопорядку [40, с. 187–197].

Довший час протиставлення кібернетичної та інформаційної безпеки мало місце в європейській та американській політико-правовій доктринах. Однак, в аналітичній доповіді «Redefining Information Warfare Boundaries for anArmy in a Wireless World» [119] від корпорації «РЕНД» на замовлення сухопутних військ (армії) ЗС США (звіт 2013 року, код звіту по проекту –

RAND10473) зазначено, що в практичній діяльності органів військового управління, суб'єктів забезпечення інформаційної безпеки інформаційне середовище необхідно розглядати як єдине середовище в двох вимірах: людському та технічному. Таким чином, позиція, що багаторазово обґрунтовувалась українськими вченими, що кіберпростір є невід'ємною частиною інформаційного простору, а відповідно кібербезпека – складовою інформаційної безпеки, почала розглядатись як можлива і на міжнародному. рівні.

Психологи розкривають її як відчуття, сприйняття, переживання необхідності у захисті життєво важливих потреб, інтересів людини. Правники – як систему встановлених законом правових гарантій захищеності особи і суспільства. Філософи кажуть. що це стан, тенденції розвитку і умови життєдіяльності соціуму, за яким забезпечується оптимальне співвідношення свободи і необхідності. Політологи вказують її як властивість системи і результат діяльності ряду органів держави; процес для досягнення поставлених завдань щодо забезпечення захищеності особи, суспільства, держави [109].

Американський соціолог, історик Іммануїл Валлерстейн задля виявлення подібності зв'язків між явищами розглядав інформаційну захищеність з урахуванням трансдисциплінарної стратегії. Він був проти створення бар'єрів щодо предмету дослідження. Сучасні методи дослідження базуються на різни світоглядних позиціях щодо соціального світу і людини [125].

Безпека з погляду філософії є формою існування. В роботах Щуровського А. М., Ященка В. Я. існування виступає по відношенню до безпеки як родове поняття, ширше за своїм змістом [103, С. 19-20].

Ліпкан В. А. стверджує, що безпека з точки зору філософії має соціальний зміст і несе риси історичності, соціальності, виступає частиною практичної людської діяльності. Поза суспільством відсутня безпека, і зміст

її залежить від тих змін, що відбуваються в організації життєдіяльності суспільства [32].

Поняття безпеки в пізнавальному філософському підході виступає інструментом пізнання сутності існування системи як цілісного організму, методологічною базою аналізу якості життєдіяльності конкретної суспільної системи, її ефективності, стійкості до різних загроз, спрямованих на порушення бажаного її стану.

Категорія «безпека» загалом характеризує стан людського суспільства, при якому не летять російські ракети по домівкам; при якому забезпечується його нормальне існування та стабільний розвиток. У світоглядному аспекті безпека є важливим питанням як наукового пізнання, так і практики існування соціуму в масштабах окремої держави та планети загалом [2].

Безпека є усвідомлене явище. Уявлення, відчуття знання, досвід про захищеність мають значущу роль у спільному житті. Усвідомлення її необхідності обумовлює глибоке розуміння сутності проблем, що виникають, реальних загроз. У основі цього поняття як системи мають місце інтереси особи, нації, держави, чи міжнародного співтовариства. Подальшого розвитку та існування соціальної системи не буде без цього.

Криштоф Лідерман, польський безпекознавець, стверджує, що безпека стосується в більшій мірі суб'єктивного відчуття [117]. Проявом багатства різноманітності людської природи, невичерпності якостей є почуття необхідності самозахисту з подальшим усвідомленням формування системи охорони та захисту. Безпека знаходить відображення у свідомості суб'єкта суспільних відносин як динамічний процес, що має низку понять – рівень розвитку системи, стан, культура, цивілізованість. В політичній, економічній, правовій, культурній сферах превалюють статистичні ознаки: визначення стану захищеності від загроз у просторі, часі та за колом осіб.

У практичній площині соціальних систем захищеність не є абстрактним явищем, відірваним від конкретних умов життя. Її зміст залежить від соціальних конкретних умов. Це потреба для існування суб'єкта будь-якого

рівня (особа, держава, т.і.) з огляду на те, що його функціонування пов’язане з задоволенням важливих потреб людини.

Дискутують у сучасній науковій літературі про те, що постановка самої проблеми безпеки пов’язується до антиподу – небезпеки чи загрози. Такий методологічний підхід обґрунтовує, якщо відсутня небезпека, то зникає потреба в безпеці, а, також, в забезпеченні існування системи охорони, протидії, захисту, оборони. Польський юрист, фахівець з міжнародного тероризму Krzysztof Liedel стверджує, що безпека і загроза є нерозривно пов’язаними явищами. Вони є протилежні одиниці виміру соціальних явищ [118].

Однак, прагнеш до миру – готуйся до війни. Це сутність іншого підходу. Безпека повинна мати місце завжди, якщо навіть небезпеки, або загрози нема. Прагнення до безпеки є виразом розумності соціальної системи, проявом усвідомленого змісту її буття, суспільного і морального сенсу. Не слід пов’язувати існування безпеки як явища виключно зі своїм антиподом – небезпекою. Вона повинна бути і збереженою від усіляких негативних втручань, негараздів, впливів тощо. Безпека виступає і як гарантія сталого розвитку будь-якої суспільної системи: набуття нею нових ознак, якостей. Концепція сталого розвитку в первинному своєму розумінні стосувалась необхідності встановлення балансу між задоволенням сучасних потреб людства і захистом інтересів майбутніх поколінь, акцентуючись на потребі в безпечному і здоровому довкіллі [112, p. 284–287]. На сьогодні основою такого розвитку визнається системний підхід та сучасні інформаційні технології, за допомогою яких є можливим моделювання різних варіантів напрямків розвитку, прогнозування їх результатів та вибір оптимальних, в тому числі з огляду на безпеку.

Захищеність (безпека) є поняттям, що окреслює стан стабільності, спокою, відсутності загрози. Охоплює задоволення таких потреб як існування, виживання, незалежність, мир, спокій, наявність і стабільність розвитку, цілісність [127, с.27].

Г. А. Пастернак-Таранушенко доходить висновку, що безпека – це стан об’єкта захисту, що відрізняється динамічною стабільність та своєчасною можливістю вплинути на хід подій з метою збереження цього об’єкта [51, с. 29]. Він спробував через теорію статики довести теорію динаміки безпеки.

На індивідуальному, суспільному, національному, міжнародному рівнях в будь-яких умовах передбачається застосування системного підходу щодо всебічного врахування багатьох факторів. Важливий фактор – обрати таку стратегію розвитку соціальної системи, за якої досягається гармонія її взаємовідносин з іншими соціальними системами на основі ідей співіснування, взаємодії, співпраці.

Таким чином, безпека – це тенденції розвитку і умови життєдіяльності соціуму, його структур, інститутів, що визначаються політичними, правовими настановами, за яких забезпечується збереження їх якісної визначеності та вільне функціонування. Також це захищеність вказаного функціонування від потенційних і реальних загроз [85, с. 278-282].

Трансформація категорії безпеки відбулась разом із визначенням довкілля, пізнанням природніх процесів, поширенням наково-технічних знань, культури. В основі розуміння безпеки лежить ідея, яка протягом століть мотивує науковців, – це ідея контролювати майбутнє, прогнозувати майбутні події та прораховувати ймовірні сценарії розвитку з максимальною вірогідністю з метою створення ідеальних умов розвитку людства [2].

Згідно енциклопедичному визначенню під категорією «інформаційна безпека» слід розуміти: – законодавче формування державної інформаційної політики;

– створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;

– підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України;

– гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; – всебічний розвиток інформаційної структури;

– захист права власності всіх учасників інформаційної діяльності в національному просторі України;

– створення і впровадження безпечних інформаційних технологій;

– охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою;

– збереження права власності держави на стратегічні об'єкти інформаційної інфраструктури України;

– створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;

– встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України 139 та порядок використання цих ресурсів на основі договорів із іноземними державами;

– захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;

– законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України [25, с. 744].

Фурашев В.М. при визначенні поняття інформаційної безпеки дотримується однієї з поширених в науковому світі позицій, яка розглядає стан захищеності життєво важливих інтересів суспільства, людини, держави. За якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невірогідної, невчасної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення

режиму доступу до інформації з подальшим її розповсюдженням та використанням [98, с. 59-66]

Позиція Дзьобаня О.П. і Пилипчука В.Г. є близькою за змістом, яка визначає інформаційну безпеку як стан захищеності життєво важливих інтересів суспільства, держави, людини в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, що забезпечує їх стабільний розвиток [15, с. 150].

Довгань О.Д пропонує розуміти під інформаційною безпекою результат управління реальними та (або) потенційними загрозами щодо захищеності важливих інтересів людини і громадянина, держави і суспільства в інформаційні сфері, використовуючи включно правові методи [12].

Цікавою є точка зору О. Логінова, який вважає, що не слід обмежуватись поняттям «стан» при визначенні категорії «інформаційна безпека», а вказує, що вона є процесом. На його думку, інформаційну безпеку слід розглядати крізь органічну єдність ознак, так як властивість, стан, управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення, мінімізації впливу негативних наслідків, включно у сфері інформаційної діяльності органів виконавчої влади [33, с.155].

Усі тлумачення категорії «інформаційна безпека» є вартими уваги. Не доцільно суворо дотримуватись однієї позиції. На нашу думку, комплексний підхід є найбільш відповідним, згідно з яким інформаційна безпека визначається через найбільш важливі функції, істотні риси, враховуючи постійну динаміку інформаційних, і соціальних систем. Отже, коли йдеться про інформаційну безпеку людини – то це насамперед потреби людини, можливість реалізації яких в правовому полі закріплюється через її права і свободи.

Очевидно, що інформаційна безпека є складним, системним явищем, на розвиток якого мають безпосередній вплив зовнішні і внутрішні чинники: а)

політична обстановка у світі; б) наявність потенційних зовнішніх і внутрішніх загроз; в) рівень і стан інформаційно-комунікаційного розвитку країни; г) внутрішньополітична обстановка в державі; е) інформаційна гігієна, обізнаність суспільства у цьому та інші [42]. Це складна, динамічна, цілісна соціальна система, компонентами якої є підсистеми безпеки, особистості, держави, суспільства. Чинників може бути безліч, з яких якісь є вагомими, деякі – менш вагомими.

Отже, з одного боку досліджуване поняття є тенденціями розвитку і умови життєдіяльності структур, інститутів соціуму. Визначається відповідними політичними, правовими та іншими настановами. З іншого боку – це захищеність вказаного функціонування від реальних і потенційних загроз [85, с. 278-282].

Таким чином, гносеологічний зміст зводиться, з однієї сторони, до небезпек і загроз, а з іншої – до можливостей суб'єктів щодо створення безпечних умов існування об'єкта інформаційної безпеки. Логічний зміст має значення в правовій площині. Нормативне закріплення правової категорії означає, що на ньому буде будуватись система інформаційної безпеки. Після закріплення у відповідних правових нормах буде виконуватись регулятивну, охоронна функції права. Тобто закладаються основи захисту об'єктів інформаційної безпеки і правого регулювання діяльності її суб'єктів.

1.2. Система національної інформаційної безпеки

Система національної безпеки України зазнавала величезних випробувань національного, регіонального, глобального рівнів в умовах гібридної війни, а тепер вже і повномасштабної агресії.

Найбільш розвинуті системи інформаційної безпеки функціонують у США, ФРН, Ізраїлі, Великій Британії [30, с. 166-168].

Важливо зауважити, що згідно ст. 3 Закону України «Про основи національної безпеки України» [75] об'єктами забезпечення національної безпеки є: 1) держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 2) суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; 3) людина і громадянин – їхні конституційні права і свободи [74].

Стаття 4 визначає, що суб'єктами забезпечення національної безпеки є: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; Національне антикорупційне бюро України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України; органи і підрозділи цивільного захисту; громадяни України, об'єднання громадян.

О.О. Тихомиров вважає, що суб'єкт забезпечення безпеки це одна з основних категорій, що використовується для розкриття змісту системи забезпечення як національної, так і інформаційної безпеки, якій традиційно приділяється багато уваги законодавцем, оскільки саме законодавство у сучасній правовій державі є засобом визначення повноважень суб'єктів [91].

Об'єктами системи інформаційної безпеки можуть бути її суб'єкти, такі як громадянин, держава, окремі її органи, інститути тощо. Власне тому, вважаємо за потрібне говорити про об'єктно-суб'єктний склад як елемент системи інформаційної безпеки.

М.Б. Левицька виокремлює: а) суб'єктів, діяльність яких безпосередньо підпорядкована завданням забезпечення відповідного рівня національної

безпеки як у комплексі (РНБО), так і на окремих напрямках діяльності (правоохоронні та інші державні виконавчі органи спеціальної компетенції); б) суб'єктів, для яких участь у забезпеченні національної безпеки є допоміжним, другорядним завданням порівняно з основною діяльністю (всі інші державні і громадські організації, наприклад, пункти охорони громадського порядку т.і.); 3) суб'єктів, для яких здійснення такої діяльності є суттєвим, але не єдиним напрямком їх діяльності (вищі органи законодавчої, виконавчої та державної влади) [29, с.66].

В теорії національної безпеки є перелік умовних двох груп суб'єктів – ті що не наділені державно-владними повноваженнями, і ті, що ними не наділені, хоча в окремих випадках можуть мати певний обсяг делегованих державно-владних повноважень. Формально виділяють дві: державне забезпечення і недержавне забезпечення [91]. О.О. Тихомиров пропонує також серед суб'єктів виділяти: міжнародні організації; держава в особі державних організацій; недержавні організації; громадяни та їх об'єднання [91].

Такий підхід закріпили в Доктрині інформаційної безпеки, яка передбачала що діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на поєднанні діяльності держави, громадянського суспільства і людини [13].

Необхідне забезпечення законодавчого захисту прав та інтересів всіх суб'єктів інформаційних відносин. Державна інформаційна політика повинна відбивати нагальні питання, що склалися у міжнародній інформаційній безпеці, тощо. Складно гармонійно забезпечити інформаційну безпеку держави, особи, суспільства з одночасним виокремленням нагальних пріоритетів. До завдань слід віднести, наприклад, створення основних точок захисту системи національної безпеки в інформаційній сфері, практичну реалізацію створення ефективної системи інформаційної безпеки, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня наслідків і рівнів їх інтенсивності. Акцент інформаційної політики

держави повинен базуватись на забезпеченні права на достовірну, повну, своєчасну інформацію, свободи слова, інформаційної діяльності в національному інформаційному простір, недопущення втручання в внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно Конституції України; вдосконалення вітчизняного національного інформаційного продукту, національно-духовних та культурних цінностей України; забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантування державної підтримки науково-технічної продукції та інформаційних технологій [4].

Чинники сили чи слабкості держави обумовлюють вибір політики національної безпеки, до яких, на думку Фредеріка Х. Гартмана, відносяться: а) демографічний (кількість населення); б) демографічна структура і тенденції (зростає чи зменшується?); в) географічний чинник (положення, розмір території, клімат, географічні особливості); г) економічний чинник (сировинна база, потреби, об'єми валового виробництва, прогнозоване господарське зростання); д) організаційно-адміністративний чинник (форма правління, ставлення суспільство до влади, ефективність діяльності влади); є) історико-психолого-соціологічний чинник (історичний досвід, ставлення до життя, єдність суспільства); ж) військовий чинник (спосіб організації і стан ефективності збройних сил, їх розмір) [114].

І.Р. Боднар розглядає національну безпеку України в інформаційній сфері як інтегральну цілісність чотирьох складових – персональної, суспільної, комерційної (корпоративної) й державної безпеки [4].

Забезпечення безпеки в інформаційній сфері деякі фахівці визначають як комплекс адміністративних заходів, необхідних для досягнення такого стану інформаційного розвитку (духовного, соціально-політичного, технічного) та захищеності суспільства, за якого сторонні інформаційні впливи не завдають суттєвої шкоди національним інтересам [53, с. 672].

Таким чином, ми розуміємо, що має створюватись сприятливий психологічний клімат в національному інформаційному просторі для утвердження загальнолюдських, національних моральних цінностей. Повинен також відбуватись технологічний розвиток, зокрема стосовно розбудови та оновлення національних інформаційних ресурсів, упровадження новітніх технологій створення, оброблення та поширення інформації. Важливо захищати інформацію, зокрема щодо забезпечення її конфіденційності, цілісності, доступності, в тому числі захист від кібернетичних атак. Це має бути зосереджена діяльність держави. громадянського суспільства та людини за цими названими напрямками вище. [53, с. 672].

Цілком очевидно, що суспільство та держава мали усвідомлювати, що найбільша небезпека йде від Росії. Тому необхідно було вже з 2014 року, або навіть з 1991 (агресія в Придністров'ї), 2008 р. (Грузія), робити рішучі дії для захисту України. Саме тому в наступному розділі цієї роботи простежимо становлення нормативного забезпечення інформаційної безпеки в законодавстві України.

РОЗДІЛ 2
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Нормативно-правове регулювання інформаційній безпеці

Базова потреба сучасної держави – створення ефективної системи інформаційної безпеки. Це вимагає розробку відповідної державної політики, її закріплення та реалізації. Передбачається пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері протидії загрозам національних інтересів та впорядкування відповідного правотворчого процесу [47, с. 132-137.].

О. В. Олійник стверджує, що система правового регулювання інформаційної безпеки в Україні включає масив правових норм, які регулюють відносини в даній сфері, правовідносини, що виникають на основі застосування правових норм, та відповідних актів [47]. Хоча можна і стверджувати, що правове регулювання насамперед може розглядатись лише як складова забезпечення інформаційної безпеки.

Цимбалюк В. В. вважає, що «забезпечення безпеки» - це тавтологічний вираз, непридатний для наукового вжитку. С.В. Мельник стверджує, що безпека та забезпечення її – різні поняття, так як безпека виражає характеристику певного стану, а забезпечення безпеки – дієву характеристику, діяльність, спрямовану на підтримання вказаного стану [40, с. 187–197].

Українські мовники схиляються до того. Що «безпеку» слід «гарантувати», а не «забезпечувати» [86]. Але вираз «забезпечувати безпеку» прийнятий в побуті, хоча і не відображає правового змісту категорії.

В англійські мові також можна сказати «to provide security». Або – «to ensure security», «to secure». У зв’язку з ратифікацією великої кількості

міжнародно-правових актів, а також з процесом євроінтеграції, виникає вплив перекладів міжнародних правових понять і сталих виразів з англійської мови. [121].

Тому, ми не будемо так загострювати увагу на цьому питання. Немає різниці, на нашу думку, чи казати «гарантувати», чи «забезпечувати». Це сталі вирази. В цій роботі буде використовуватись словосполучення «забезпечення безпеки» і його похідні.

На думку деяких дослідників правову основу забезпечення інформаційної безпеки України є закони України "Про основи національної безпеки України", "Про інформаційну безпеку України", "Про доступ до публічної інформації", "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки", інші закони та інформативно-правові акти, Конституція України, ратифіковані Україною Договір про безпеку і співробітництво в Європі, Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов'язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах [38, с. 13-20].

Хоча і названі акти становлять важливу частину законодавства щодо інформаційної безпеки, але водночас виявились не ефективними, не достатніми для того самого стану безпеки. Закон України «Про інформаційну безпеку України» на жаль не існує, незважаючи на об'єктивну потребу такого акту в час, коли Україна була в стані гібридної війни з 2014 року. За умов, коли інформаційна безпека є найбільш атакованою і, водночас, найбільш вразливою. Враховуючи факти, що Росія, країна-терорист, поширювала активно пропаганду на своїх нікчемних національних телеканалах (та інших джерелах, напр.., кіноіндустрія) проти українців ще у 2010-х, та й, навіть в 2000-х. В кіноіндустрії Росії хибні стереотипні

постулати поширювались щодо українців створювались взагалі завжди, починаючи з 20 століття. Ба навіть забороняли українцям робити своє україномовне кіно.

Інформаційна безпека не є винаходом останніх десятиліть. Досліджуючи правове забезпечення інформаційної безпеки, слід звернути увагу на те, що його становлення і розвиток нерозривно пов'язаний з правовим регулюванням інформаційних відносин, яке містить значну кількість норм, що безпосередньо чи опосередковано стосуються об'єкту дослідження. Усвідомлення значимості інформаційної захищеності в історії людства змінювались з усвідомленням суспільної цінності інформації, проникнення інформаційної діяльності в усі сфери життєдіяльності суспільства, життя людини, держави [19, с. 63-66; 20].

В Україні 13 грудня 1991 р. було прийнято Закон України «Про основи державної політики у сфері науки і науково-технічної діяльності». Цей закон мав на меті створення правових основ державної політики у сфері науки і науково-технічної діяльності, а також визначав правові, організаційні та фінансові засади функціонування і розвитку науково-технічної сфери, забезпечення потреб суспільства і держави у технологічному розвитку. В ньому було закладено підвалини для розвитку інформаційного суспільства, про яке на момент початку розбудови держави особливо ніхто не замислювався. Чудово, що тоді було сформульовано все-ж таки прагнення нації до розвитку. Цей Закон виглядає як передвісник становлення і розбудови інформаційного суспільства і суспільства знань, як його наступного етапу.

2 жовтня 1992 р. був прийнятий Закон України «Про інформацію», який був прийнятий на підставі Декларації про державний суверенітет України та Акта проголошення незалежності України [48]. На законодавчому рівні закріпили принципи інформаційних відносин та напрями державної інформаційної політики в цьому законі. Основними принципами інформаційних відносин визнано: - гарантованість права на інформацію; -

відкритість, доступність інформації, свобода обміну інформацією; - достовірність і повнота інформації; - свобода вираження поглядів і переконань; - правомірність одержання, використання, поширення, зберігання та захисту інформації; - захищеність особи від втручання в її особисте та сімейне життя.

А основними напрямами державної інформаційної політики визначались: - забезпечення доступу кожного до інформації; - забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; - створення умов для формування в Україні інформаційного суспільства; - забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; - створення інформаційних систем і мереж інформації, розвиток електронного урядування; - постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; - забезпечення інформаційної безпеки України; - сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Цей акт був важливим. Після того, як УРСР була в ізоляції довгий час, українська держава і суспільство опинились посеред бурхливих інформаційних процесів, які вимагали від України формування власних пріоритетів і напрямів розвитку інформаційної сфери. Прийняття цього Закону стало знаковою подією в організації безпечного інформаційного простору молодої держави. Були визначені поняття інформації, її види та галузі; принципи інформаційних відносин; пріоритетні напрями державної інформаційної політики; режими доступу до інформації; гарантії права на інформацію; основні види інформаційної діяльності; питання охорони інформації; підстави відповідальності за делікти в інформаційній сфері; процедура інформаційного запиту; коло учасників інформаційних правовідносин, їхні права та обов'язки; правові форми міжнародного співробітництва в галузі інформації; гарантії інформаційного суверенітету

України [55, с. 64-68]. Цей закон мав звісно недоліки, але згодом його редагували.

На основі та на реалізацію положень цього закону було прийнято цілу низку законів, що стосувались окремих видів інформаційних відносин, зокрема: «Про друковані засоби масової інформації (пресу) в Україні» (від 16 листопада 1992 р.) [80], Закон України «Про науково-технічну інформацію» (від 25 червня 1993 р.) [74], «Про охорону прав на винаходи і корисні моделі» (від 15 грудня 1993 р.) [59], «Про телебачення і радіомовлення» (від 21 грудня 1993 р.) [79], «Про авторське право і суміжні права» (від 23 грудня 1993 р.) [60, с.64], Про державну таємницю» (від 21 січня 1994 р.) [67], «Про національний архівний фонд і архівні установи» (від 24 грудня 1993 р.) [71], «Про захист інформації в автоматизованих системах» (від 5 липня 1994 р.) [Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 р. №81/94-ВР; (зі змінами 2013 р. Про захист інформації в інформаційно-телекомунікаційних системах). ВВР України. 1994. № 31. Ст.286.], «Про зв'язок» (від 16 травня 1995 р.) [82], Закон України «Про бібліотеки і бібліотечну справу» (від 27 січня 1995 р.) [61], «Про рекламу» (від 3 липня 1996 р.) [77], «Про систему Суспільного телебачення і радіомовлення України»(18 липня 1997 року) [78], «Про Національну раду України з питань телебачення і радіомовлення» (від 23 вересня 1997 року) [73], «Про державну підтримку засобів масової інформації та соціальний захист журналістів»(від 23 вересня 1997) [66, с. 302] та інші.

В Україні за всі роки незалежності все ще не прийнято закону, який би визначав концепцію державної інформаційної політики. На законодавчому рівні неврегульованим залишається і забезпечення інформаційної безпеки. Декілька спроб ухвалити концепцію державної інформаційної політики на законодавчому рівні - 2002, 2009, 2010 та 2011 рр.

Конституція України окреслює повноваження суб'єктів, відповідальних за її забезпечення - Рада національної безпеки і оборони

України; Президент України; Верховна Рада України; Кабінет Міністрів України та інших.

В 1998 році було прийнято два закони, що стосувались інформатизації - Закон України «Про Національну програму інформатизації» [72], Закон України «Про Концепцію Національної програми інформатизації» [70], які на законодавчому рівні створили передумови для забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної та інших сферах. Протягом наступних років було прийнято кілька законів, що заклали основу для формування телекомунікаційного законодавства України.

В 2003 році було врегульовано на законодавчому рівні питання електронного документообігу. Було прийнято закони «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг». Вони створили підґрунтя для розвитку інфраструктури електронного документообігу [68; 69].

Отже, структура законодавства України може брати приклад з іншої країни, і потребує врахування реалій українського законодавства і правової системи. Тим не менш, обґрунтованою вбачається позиція Олійника В.Д., щодо включення положень щодо інформаційної безпеки на всіх рівнях законодавства.

В.Д. Олійник, обґрунтовуючи у своїй праці, вважає включення положень щодо інформаційної безпеки на всіх рівнях законодавства є важливим. До цього слід прислухатись. Положення про неї повинні органічно включатися у всі рівні законодавства, в тому числі і в конституційне законодавство, основні загальні закони, закони щодо організації державної системи управління, спеціальні закони, відомчі правові акти тощо [47, с.137].

Зазначимо, що правове забезпечення інформаційної безпеки має поєднувати норми щодо:

– правового закріплення національних інтересів людини, суспільства і держави у інформаційній сфері;

– форм участі громадянського суспільства у забезпеченні інформаційної безпеки;

– суб'єктивних інформаційних прав людини та громадянина;

– системи органів, відповідальних за забезпечення інформаційної безпеки.

Отже дві стратегії національної безпеки України, що були розроблені у 2007 і 2016 рр. У Стратегії 2007 зазначалось, що посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності; недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту; наближається до критичного стан безпеки інформаційно-комп'ютерних систем у галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій.

Ця Стратегія була відредагована в 2012 році. Ці положення, що описали вище. Зникли. Проте серед завдань політики національної безпеки у внутрішній сфері з'явився підрозділ, присвячений забезпеченню інформаційної безпеки. Передбачалось виробництво конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів; впровадження новітніх інформаційних технологій; забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони, кредитно-банківської сфери, систем управління об'єктами критичної інфраструктури; впровадження гармонізованих із відповідними стандартами держав-членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність; створення національної системи кібербезпеки.

Дана Стратегія відокремлює сферу інформаційної безпеки від кібербезпеки і безпеки інформаційних ресурсів. До загроз України віднесено ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. До загроз кібербезпеці і безпеці інформаційних ресурсів – уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших виді інформації з обмеженим доступом.

Пріоритетами забезпечення інформаційної безпеки згідно Стратегії 2018 року визначено: забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм інформаційної агресії; протидія інформаційним операціям проти України, маніпуляція суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; створення системи оцінки інформаційних загроз та оперативного реагування на низ; виявлення суб'єктів українського інформаційного простору, що створено та/або використовуються росією для ведення інформаційної війни проти України та унеможливлення їхньої підривної діяльності; упровадження загальнонаціональних освітніх програм з медіа культури із залученням громадського суспільства та бізнесу.

А пріоритет забезпечення кібербезпеки і безпеки інформаційних ресурсів – створення системи забезпечення кібербезпеки, мережі реагування на комп'ютерні надзвичайні події [CETR]; моніторинг кіберпростору з метою своєчасного виявлення, запобігання і їх нейтралізації; розвиток інформаційної інфраструктури держави; відмова від програмного забезпечення, зокрема антивірусного, розробленого у Росії; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, враховуючи практики держав-членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів

сектору безпеки і оборони; розвиток міжнародного співтовариства у сфері забезпечення кібербезпеки, інтенсифікації співпраці України та НАТО.

В 2008 році тогочасним президентом було введено в від дія рішення РНБО «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» [74]. На виконання цього указу РНБО було розроблено проект Доктрини інформаційної безпеки України – сукупності основних офіційних поглядів на мету, задачі, принципи й основні напрямки забезпечення інформаційної безпеки держави. Доктрина була затверджена Указом Президента у липні 2009 р. В обговоренні і підготовці документу задіяли понад 30 органів державної влади, наукових установ, враховано понад 200 конкретних пропозицій, у тому числі від представників громадських організацій, експертного середовища [13].

Основна мета її – створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету. Доктрина втратила чинність відповідно до Рішення РНБО України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [81], яким також передбачено розробку ряду законодавчих актів, зокрема, Стратегії розвитку інформаційного простору України, Стратегії кібернетичної безпеки України, проекту Закону України про кібернетичну безпеку України. Станом на 2017 рік було розроблено і введено в дію Указом Президента України лише Стратегія кібернетичної безпеки України [88], інші ж акти проходять різні етапи розробки – від проектної роботи до експертної оцінки і погодження в комітетах ВР, проте так і не були винесені на розгляд. Це - дивно і прикро.

При РНБО є міжвідомча комісія з питань інформаційної політики та інформаційної безпеки. Її завдання включать аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики. Як варіант, можливо розглянути розширення повноважень зазначеної структури, в тому числі включення завдання координації [87].

Указом Президента України була затверджена Доктрина інформаційної безпеки України на основі вищезгаданої Стратегії національної безпеки України, а також Конституції і законів України та міжнародних договорів України. Метою доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв'язаної нею гібридної війни. Доктрина інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Не простим завданням на даний момент буде оцінка ймовірного впливу цього документу на українські реалії інформаційної сфери. Основними суб'єктами повноважень згідно неї стали Кабінет міністрів, Служба безпеки України, Державне агентство України з питань кіно, Міністерство інформаційної політики, Міністерство культури України, Міністерство закордонних справ, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, розвідувальні органи, Державна служба спеціального зв'язку та захисту інформації, Національний інститут стратегічних досліджень; і також РНБО як орган, що здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. В цій Доктрині інформаційної безпеки суттєво посилені та конкретизовані повноваження Міністерства інформаційної політики.

З перших рядків Доктрини відразу стає очевидно, що цей документ є однобічним, тому що не враховує застосування РФ технологій гібридної війни проти України, яка перетворило інформаційну сферу на ключову арену протиборства. «Саме проти України РФ використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України». Джерело загрози і напрям

протидії цим документом визначили. На нашу думку, це актуально на той час було при гібридній війні, але такі «точкові» документи за відсутності правового регулювання питань інформаційної безпеки були недостатніми.

Також, є чинним досі Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 роки», яким ще в січні 2007 року було визначено одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя [76]. Цим законом було вперше законодавчо закріплено поняття «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави.

Таким чином, аналіз становлення законодавства у інформаційній сфері в цілому дає розуміння, що інформаційне законодавство України формувалось безсистемно, ситуативно, і під впливом різних моделей правового регулювання інформаційної сфери. Україна прагне, щоб українське законодавство відповідало до рівня ЄС. І над цими будуть працювати відповідні фахівці. Після звільнення території, окупованих росіянами, важливим є опрацювання базового закону – Інформаційного кодексу, який би відображав основні пріоритети, визначав систему і структуру інформаційного законодавства, водночас, залишаючи простір для реагування на динамічні процеси в інформаційній сфері. Технологічний розвиток відбувається стрімкими темпами, а, отже, вимагає таких же темпів правового і організаційного забезпечення питань, що пов’язані з виникненням нових соціальних відносин.

Очікувалось, що впровадження Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки дасть можливість забезпечити позитивні зміни в життєдіяльності суспільства і людини, а саме:

підвищити рівень інформаційної безпеки людини, суспільства, держави, ступінь розвитку інформаційно-телекомунікаційної інфраструктури, зокрема українського сегменту Інтернету; сприяти розвитку демократії; збільшити рівень захисту прав і свобод людини та її добробуту; активізувати участь громадян в управлінні державою; забезпечити перехід економіки до моделі науково-технічного та інноваційного розвитку; створити нові робочі місця; підвищити конкурентоспроможність України, ефективність державного управління, продуктивність праці у всіх сферах економіки, тощо.

Але складна політична і економічна ситуація, а також низка інших чинників, такі як недостатнє забезпечення доступності якісних адміністративних послуг суб'єктам інформаційного суспільства та гарантій їх відповідності затвердженим державним вимогам; відсутність чіткого розмежування повноважень органів державної влади та органів місцевого самоврядування, координації їх діяльності в цій сфері; недостатній рівень урахування світового досвіду у сфері розвитку інформаційного суспільства; тощо, призвели до невиконання в Україні низки положень цього Закону та заходів, запланованих Кабінетом Міністрів.

Про низькі темпи розвитку інформаційного суспільства свідчить також індекс мережевої готовності (Networked Readiness Index), що визначає рівень розвитку ІКТ у країнах світу. Україна в 2015 році посіла 71 позицію серед 143 країн світу у рейтингу за рівнем розвитку інформаційно-комунікаційних технологій (ІКТ). Найвищу рейтингову позицію за Індексом мережевої готовності Україна продемонструвала у 2009 році (62 місце). Після цього упродовж двох наступних років було втрачено 28 пунктів, внаслідок чого у 2011 році наша країна перемістилася на 90 позицію серед 138 країн світу. Причиною досить низьких позицій України у світовому рейтингу 2017 року є відставання за складовими, що характеризують політичне і регуляторне середовище – 122 позиція та низький рівень використання ІКТ урядом – 124 позиція [8].

Зазвичай ці закони ухвалювались ситуаційним підходом. О. Г. Марценюк виокремлює такі: а) відсутність легальної, чіткої, ієрархічної єдності законів, що призводить до суперечливого тлумачення та застосування норм права на практиці; б) значна кількість законів та підзаконних нормативних актів в сфері інформаційних відносин ускладнює пошук, аналіз і узгодження; в) нові правові акти часто неузгоджені з раніше прийнятими, що призводить до правового хаосу [39, с. 38].

Заслуговує на увагу позиція В. А. Ліпкана, який зауважив, що «…в інформаційному законодавстві відсутній чітко сформульований склад багатьох правопорушень, а також не виділено ознаки, за якими ті чи інші інформаційні правопорушення мають бути згруповані до однієї глави. Зокрема відсутні напрацювання щодо таких актуальних питань як: інформаційні конфлікти, інформаційно-правовий компроміс, інформаційно-правова відповідальність, інформаційна деліктологія, інформаційна функція держави тощо [21, с. 5-11.]. Очевидно зауважити, що кількість Законів в інформаційній сфері не переростає в якість. Подібний хаос, на жаль, панує в багатьох інших сферах законодавства України.

Красноступ Г.М. зауважила «…нам не потрібно створювати нові закони у сфері інформації, а систематизувати вже існуючі, визначаючи у них правові гіперзв’язки з метою подальшого їх кодифікування на рівні Кодексу України про інформацію» [26]. Однак, інформаційна сфера розвивається швидко, і потребує в регулюванні нових суспільних відносин постійно.

Максименко Ю.Є пропонує кодифікацію українського інформаційного законодавства задля його покращення, і стверджує, що воно потребує узгодження з європейськими стандартами [36, с. 20]. Це очевидно, тому що майбутнє України – в ЄС.

Отже, проаналізувавши законодавство в інформаційній сфері в цілому дозволяє зробити висновки, що інформаційне законодавство та законодавство в інформаційній безпеці знаходиться на етапі становлення.

Виокремлюють наступні умовні етапи: I. 1992 -1996 роки – становлення основ інформаційного законодавства; II. 1996-2003 роки – усвідомлення і формулювання основ інформаційної безпеки як складової національної безпеки; III. 2003-2014 роки – усвідомлення розвитку глобального інформаційного суспільства, приєднання до міжнародних актів щодо у сфері інформаційного суспільства, права і безпеки, розвиток національного законодавства згідно з тенденціями міжнародного права. До речі, ми вважаємо, що у 2010-2014 роках була криза у сфері інформаційної безпеки, обумовлена незваженою інформаційною політикою держави; IV. 2014 – донині – розвиток законодавства у сфері інформаційної безпеки, спрямований на посилення позицій України у гібридній війні; V. 2022 – донині – розвиток законодавства і розробка законів вже під час воєнного стану.

2.2. Класифікація загроз України та наслідки інформаційних впливів

Класифікація загроз дозволяє визначити, які саме загрози становлять переважний пріоритет в науковій, чи нормативно-правовій перспективі. Згідно Закону України «Про основи національної безпеки України» до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп’ютерна злочинність та комп’ютерний тероризм; прояви обмеження свободи слова та доступу громадян до інформації; розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави [75].

Згідно редакції 2017 року актуальними загрозами України в інформаційній сфері визначили: здійснення інформаційних операцій підриву обороноздатності, деморалізацію особового складу ЗСУ та інших формувань; провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації; недостатній рівень медіа-культури суспільства; розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведення державою-агресором інформаційних операцій для створення негативного іміджу України у світі; інформаційна експансія держави-агресора та контрольованих нею структур на території України та інших держав; інформаційне домінування держави-агресора на тимчасово окупованих територіях; недостатня розвиненість національної інформаційної інфраструктури; неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері; невизначеність стратегічного наративу; пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [15].

Професор В. Ліпкан класифікує загрози: а) за походженням - природне, техногенне, антропогенне; б) за ступенем гіпотетичної шкоди - загроза та небезпека; в) за повторюваністю - повторювані та продовжувані; г) за ймовірністю реалізації - вірогідні, неможливі, випадкові; д) за структурою впливу - системні, структурні та елементні; за об'єктом впливу – особа, суспільство, держава [32, с. 576]. В іншій праці запропоновано такі види загроз інформаційній безпеці: збій в роботі самого обладнання; розкриття інформаційних ресурсів; порушення їх цілісності **[**32, с. 576**].**

Чинний Закон „Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки» визначає такі загрозами інформаційній безпеці: несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації; неповноту, невчасність та невірогідність інформації; негативний

інформаційний вплив; негативні наслідки застосування інформаційних технологій [76].

Ми є свідками того, як ведеться інформаційний вплив спрямований на свідомість осіб, груп людей, і цілих держав. Психологічний вплив зазвичай здійснюється за допомогою ЗМІ, а підставлю для використання такого впливу є поверховість і легкість сприйняття. Створення ботів, масованих інформаційних атак, фейків, як свідчать реалії війни, є дієвими інструментами для дезорієнтації суспільства, маніпулювання. залякування, паніки. Спеціальні інформаційні ресурси привчають людину бездумно сприймати інформацію, вірити в неї.

Інформаційні впливи є невід'ємною складовою життєдіяльності людини в інформаційному середовищі, необхідною умовою існування суспільної та індивідуальної свідомості, формування людини та її нормальної життєдіяльності, а потреба в інформації – базовою потребою особистості. Достатність інформаційних впливів на свідомість забезпечує образ реальності, когнітивну модель світу і ситуації, розуміння себе і своїх можливостей.

За результативністю інформаційні впливи поділяють на ефективні й неефективні; сутнісні, істотні, глибинні й неістотні, поверхневі; стабілізуючі та дестабілізуючі; організуючі та дезорганізуючі. За масштабом трансформацій, спричинених впливами, їх поділяють на глобальні, локальні та часткові.

Перечислимо наступні наслідки інформаційних впливів:

1. Психофізіологічні ефекти (зміна пульсу, кольору шкіри, тиску, гормонального складу крові, частоти дихання, тощо).

2. Емоційні ефекти (зміна емоційного стану, поява одних та зникненні інших почуттів, поява імпульсів до активних роздумів, до переробки, трансформації інформації; виникнення прагнення до отримання чи створення нової тощо).

3. Поведінкові ефекти спостерігаються у вигляді певних дій, вчинків, відповідної поведінки у сфері предметної діяльності (зокрема, її організації), міжособистісної взаємодії та взаємодії із самим собою

4. Когнітивні ефекти проявляються у зміні рівня поінформованості, збільшенні обсягу знань (усвідомлювано і неусвідомлювано); формуванні нових когнітивних схем, способів осмислення дійсності, оперування інформацією.

5. Ціннісні ефекти (формування нових чи зміцнення/послаблення наявних інтересів, оцінок, смаків, ставлень, ціннісних орієнтацій, настанов стосовно світу, окремих предметів, явищ, стосовно інших людей або самих себе) [106].

Проблеми збереження психічного здоров'я громадян України залишаються поза увагою держави. А в світі приділяється значна увага інформаційній гігієні і інформаційній культурі. Має бути право психічно здорової людини зберегти своє здоров'я за будь-яких умов життєдіяльності

Отже, необхідно якимось чином регулювати інформаційні потоки. Надлишок інформації спричиняє інформаційний шум. Дане явище не є безневинним. Зайва, «фонова» інформація, відволікаючи увагу людини від поставлених цілей, сприяє виснаженню його інтелектуальних сил, підвищує енергетичні витрати. Не залишається при цьому людині ні часу. ні місця для роздумів про життя. Як зазначає Томас Еріксен, "найнеобхідніше вміння в інформаційному суспільстві полягає в захисті себе від 99,99 % пропонованої інформації, якої людина не хоче" [16].

Крім того, важливим елементом інформаційної культури є інформаційна стійкість. Україна геополітично увесь час знаходиться на межі кількох потужних культурних традицій. З одного боку, в Україні ми маємо західні цінності, що є дуже добре. З іншої сторони, на превеликий жаль, знаходиться Росія, держава-спонсор тероризму, яка несе з собою пропаганду, геноцид, мародерство, тощо. Їхня інформаційна пропаганда призвела до дестабілізації регіонів, чвар, ворожнечі, та інших проблем. Згодом ця країна

почне гібридну війну, і повномасштабне вторгнення, чинячи геноцид, мародерство, окупації територій. В України – дуже жахливий сусід.

2.3. Особливості правового забезпечення прав і безпеки окремих категорій осіб інформаційній сфері

Привертає увагу статистика того, що доступ до Інтернету в країнах Скандинавії перевищує показник у 90 % населення, тоді як в Україні й інших пострадянських країнах цей показник коливається біля позначки 50 % населення [126], причому більшість – це мешканці великих міст. Згідно з даними Інтернет Асоціація України (опубліковано на їхньому офіційному сайті у квітні 2017 року), які представляють результати опитування, проведеного протягом лютого 2017 року, на початку року 64,7% дорослого населення України користуються Інтернетом. Частка користувачів Інтернет серед людей 15-29 років в Україні сягнула 97%. Зведені дані, опубліковані аналітичною ініціативою DataReportal у січні 2021 року, показали, що при загальній чисельності населення 43,6 мільйона в Україні є 29,47 мільйона індивідуальних користувачів Інтернету, що становить 67,6 відсотка проникнення [5]. Наразі майже всі села, СМТ, міста мають доступ до Інтернет-мережі, та телефони.

Будь-яка технологія може бути використана в обидві сторони. Конрад Лоренц писав, що «Є вагомі підстави вважати внутрішньовидову агресію найбільш серйозною небезпекою, яка загрожує людству в сучасних умовах культурно-історичного і технічного розвитку» [34].

Тому особливого значення набуває питання мови ворожнечі ще й під час інформаційних війн і повномасштабного вторгнення РФ. Росії буде грати на руку, якщо в нас будуть внутрішні конфлікти. Але цього, на щастя, не станеться, бо українські наразі єдині, як ніколи. Проте, знецінювати загрозу

не слід. Мова ворожнечі – це інструмент маніпуляцій із метою розколу суспільства, це елемент його дестабілізації й зменшення довіри. Буде помилкою недооцінювання негативного впливу таких явищ і проявів агресії на суспільну свідомість. У світлі цього окремо варто виділити питання відповідальності за поширення мови ненависті в публічному інформаційному просторі, точніше, її відсутності [105].

Відповідно, важливою складовою державної інформаційної політики і необхідною умовою гарантування інформаційної безпеки людини, захисту її інформаційних прав та свобод є мовне питання та його правове врегулювання [49].

Неможливо також закривати очі на небезпеки для дітей в мережі Інтернет. Англійська дослідниця С. Лівінгстон, підкреслюючи, що один з трьох користувачів Інтернету є дитиною, наголошує, що із зростанням технологій дитячі організації, представники приватного сектору, регулюючі органи мають опікуватись тим, що права дітей потребують такої ж реалізації онлайн, як і оффлайн. Права дитини, викладені в Конвенції ООН прав дитини, дослідниця застосовує до «онлайн» середовища.

Серед загроз з якими дитина може зіткнутись при використанні комунікаційних технологій можна виокремити такі: технологічні: загроза як для дітей, так і для дорослих користувачів; доступ до інформації з неприйнятним (часто незаконним) змістом, зокрема, порнографічні, такі, що пропагують наркотики, психотропні речовини й алкоголь, тероризм і екстремізм, ксенофобію, сектантство, національну, класову, соціальну нетерпимість, нерівність, асоціальну поведінку, насилля, агресію, суїцид, азартні ігри, інтернет-шахрайство [31, с. 48]; розголошення персональних даних та іншої конфіденційної інформації, як власної, так і членів сім'ї, друзів чи знайомих; контакт з незнайомцями, що може призвести наслідків як у віртуальному (кібурбулінг, дитяча порнографія тощо), так і реальному житті (сексуальне використання, фізичні ушкодження, викрадення).

Маленька дитина може дивитися більше 500-1600 реклам на день по телевізору, або (і) на платформі Youtube, дивлячись мультики через телефон, тощо. При цьому, вона не фільтрує інформацію, як дорослі, а все це відкладає в голові. Це є також небезпечно, і принаймні батькам, якщо не державі, необхідно це регулювати [115].

Діти часто страждають від боулінгу ще й в онлайні. Кібер-буллінґ (cyber-bullying), віртуальний терор, із спорідненими значеннями: агресивно нападати, задирати, прискіпуватися, провокувати, дошкуляти, тероризувати, цькувати. В українському молодіжному сленгу є дієслово аналогічного походження – «бикувати» [24].

Бесіди з київськими підлітками підтверджують наявність більшості описаних типів поведінки в їхньому досвіді чи уявленнях. Навіть хепіслепінґ, який виник відносно нещодавно, трапляється серед українських дітей [44, с.34].

Аналіз листів МОН та регіональних органів виконавчої влади у сфері освіти, зміст яких присвячений проблемам інформаційної безпеки: Лист МОН України № 1/9–768 від 06.11.09 «Про захист дітей та молоді від негативних інформаційних впливів», Лист МОН України № 1/9- 916. від 28.12.09 «Про проведення дня безпечного Інтернету», Лист МОН України № 1/9-815. від 11.11.10 «Про проведення конкурсу «Онляндія в моїй школі» свідчить про їх популістський і декларативний характер. Після перемоги державі слід в співпраці з країнам ЄС розробляти проекти для безпеки людей в «онлайн» просторі. Слід переймати досвід країн «Заходу».

Таким чином, реалізація принципу свободи інформації в суспільстві значною мірою також залежить від того, наскільки послідовно вона дотримується загальнолюдських норм і принципів, етичного кодексу поведінки. До основних етичних принципів спілкування належать: гуманізація і демократизація відносин; повага до співрозмовників і самоповага; соціальна справедливість і толерантність; суверенність

особистості (недоторканність гідності кожного); неупереджене ставлення до партнерів по спілкуванню; врахування інтересів співрозмовників, тощо

Не менш важливою є духовна сфера суспільства, складовими якої є не лише релігійність, а, насамперед, суспільна свідомість, громадська думка і соціально-психологічний клімат (у тому числі системи освіти і виховання, системи масової інформації, що впливають на соціальну поведінку та організацію життєдіяльності людей).

Також важливо значення має небезпека соцмереж, програмного забезпечення, та інших інтернет-інструментів, зокрема російського виробництва. Так Російські соціальні мережі «Вконтакте», «Одноклассники» і «Мой Мир» входять до п'ятірки найбільш відвідуваних соціальних мереж у багатьох державах пострадянського простору. Це є небезпечно! Для росіян це є «золотою жилою» щодо доступу до персональних даних. В цих соціальних мережах, наприклад, є різноманітні квести («Перевір своє знання географії», «Який у тебе словниковий запас», «Визнач свій психотип» тощо) і конкурси («Яка машина тобі личить», «Як ти будеш виглядати через 50 років», «На якого звіра ти подібний», тощо). «Безневинні» розваги дозволяють легально стежити за особою, отримувати інформацію про її вподобання, геолокацію, друзів, активність, тощо. Держави по різному реагують на цю загрозу. Від заборони окремих ресурсів російського виробництва (Молдова) до повного ігнорування (Білорусь, Казахстан, Азербайджан), або до спроб створити чи посилити вплив власних альтернативних ресурсів (Вірменія, Грузія).

Україна вже має досвід щодо намагання обмежити доступ до російських інформаційних і комунікаційних ресурсів шляхом зобов'язання провайдерів зробити їх технологічно недоступними. Указ Президента від 15 травня 2017 року № 133/2017 щодо затвердження рішення Ради національної безпеки і оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 28 квітня 2017 року викликав бурхливу реакцію громадськості і поставив низку питань щодо його законності, правомірності, допустимості в демократичному

суспільстві, а також результативності. Однак, ми раді, що було прийняте це рішення. Наприклад, в США заборонили китайський додаток «ТІКТОК», і нічого страшного не відбулося. Сьогодні українці звикли користуватися додатками компанії МЕТА, Телеграмом, Вайбером. Майже ніхто не користується російськими.

Навіть, не можна користуватись їхнім програмним забезпеченням, браузерами. Нещодавно, група дослідників виявила, що пошуковий інструмент «Яндекс» не вибиває при пошуку геноцид в Бучі, скоєний росіянами. В Twitter мережі здійснялися обговорення, і засудження компанії, що вони співпрацюють з Росією. Після цього «Яндекс» виправив цю проблему [121]. Також були скандали щодо того, що російський пошуковий інструмент «Яндекс» збирає данні про користувачів, і т.і. Тому, краще користуйтеся Google пошуком.

На жаль, і компанія «МЕТА» з своїми Фейсбуком, Інстаграмом – не є безневинними. Німецькі правозахисники у галузі захисту приватності інформації вимагали видалити кнопку “Like” в Фейсбуці. Вони заявили, що використання кнопки «Like» суперечить німецькому та європейському законодавству, оскільки як наслідок інформація про користувачів – інтереси, тривалість перебування на тій чи іншій сторінці, переходи з одного сайту на інший надходить до США, де згодом використовується для таргетування реклами, аналізу поведінки користувачів на сайті тощо. Представники соціальної мережі підтвердили, що, натискаючи цю кнопку, така інформація як ІРадреси, могла передаватися. Вони також зазначили, що ці дані, відповідно до європейського законодавства через 90 днів видаляються [45].

Одним із головних напрямків боротьби із шахрайством, зазначеним у Постанові НБУ №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28 вересня 2017 року, є впровадження банками основних технічних систем [57].

Не можливо не згадати про скандал під час виборів в США і компанії Facebook, яка збирала данні незаконно про електорат. В серпні 2022 українці

були обурені через те, що «Істаграм» заблокували сторінку Асоціації родин захисників "Азовсталі".

Також на платформах Instagram, Youtube помічений сліди росіян. Ці компанії також попали під вплив російської пропаганди, або(і) були підкуплені російською терористичною владою, в чому я не сумніваюсь. Заборонено авторам цифрового контенту в Youtube, Instagram говорити слово «русня». За це можуть заблокувати відео, чи пост.

До того ж, було помічено, що українцям в Instagram показували пости з тегом “Russia is a terrorist state”, а західним країнам – набагато менше, якщо зовсім не ховали від них [46]. Не можна також було в Instagram про геноцид в Бучі, тощо. Що ж, українці з цим безладом борються. Найменше, що ми робимо – це публічний розголос у інформаційному просторі. Дуже добре це виходить у Twitter мережі. Українці – молодці.

За оцінками експертів серед галузей, які найбільше потерпають ся від кіберзлочинців, які найбільше страждають від кіберзлочинців, перше місце займає банківський сектор, друге – енергетичний та добувний сектор, третє – телекомунікаційний. У 2017 році від фітингових атак найбільше шкоди зазнали 51,7% банків в порівнянні з платіжною системою та електронною комерцією – представниками фінансового сектору [123]. Банки мають вирішити проблему, попереджуючт якимось чином шахрайські, незаконні дії. Найчастіше клієнти банків потерпають від шахрайства. Це знижує довіру до фінансових інститутів, та мотивує шукати альтернативні способи для зберігання коштів.

Так, нагальною потребою після перемоги, на нашу думку, є розробка і прийняття базових для правового забезпечення інформаційної безпеки закону «Про інформаційну безпеку». При цьому важливим вбачається не відокремлювати кібербезпеку від інформаційної безпеки. Удосконалення методів шахрайств і збільшення частити кібератак призводить до збільшення втрав банків та їх клієнтів. Банківська система часто не встигає за швидкими темпами модернізації способів та інструментів шахраїв. Рівень протидії,

зрештою, поступається рівню зростаючих загроз. Згідно статистичними даними ЕМА (Українська міжбанківська асоціація членів платіжних систем), сума збитків громадян внаслідок дій шахраїв із платіжними картками у 2017 році склала 670 млн. грн., що перевищує попередні роки – 339 млн.грн (2016 р.), 181 млн. грн. (2015 р.), 90 млн. грн. (2014 р.) [88].

Не слід залишати поза увагою те, що інформаційна безпека, це не лише кібербезпека і не обмежується безпечним перебуванням у віртуальному просторі. Реалізація численних прав і свобод людини в сучасному суспільстві залежить від гарантування дотримання її інформаційних прав. Зокрема, це стосується права на рівень життя, необхідний для їх розвитку, права людей на вираження своїх поглядів, право на існування власного майна, на свободу думки, совісті і релігії, асоціацій і мирних зборів, доступ людини до поширення інформації, освіту, користування рідною мовою і культурою, сповідування своєї релігії, відпочинок і дозвілля.

Таким чином, свобода, що є найважливішою умовою буття людини, обумовлює необхідність гарантування інформаційної безпеки людини. Людина, який би в неї фільтр не був, має приймати рішення, будучи в безпечному адекватному інформаційному просторі. Загрози інформаційній безпеці людини є складним ієрархічним утворенням з множиною різнорівневих зв’язків. Інформаційна безпека людини базується не лише на її захищеності від інформаційних загроз, але й передбачає можливість людини як біологічного організму і соціальної істоти функціонувати, розвиватись. Авжеж, в умовах інформаційного суспільства можливості реалізації прав і свобод людини суттєво залежать від адаптованості до них самої особи, інститутів суспільства і держави, а також системи права. Необхідною складовою такої адаптації і умовою реалізації та захисту прав і свобод людини є високий ступінь інформаційної та правової культури. І ці загрози необхідно досліджувати «в ногу» з розвитком технологій.

Були розглянуті інформаційні впливи та наслідки для психіки людини. Також наведено класифікацію інформаційних загроз для України. В сфері

захисту дітей уряд України має приділяти також увагу. Це є важливо для майбутнього країни. Є багато загроз в інтернет-мережі для дітей. включаючи кібербулінг, тисячі реклам, незаконні матеріали, тощо.

Повинні впроваджуватися мовна політика, врегулювання питань пов'язаних з використанням «мови ненависті», а також побудова ефективної системи комунікації та формування публічного простору, засобів і центрів комунікації, як необхідної умови громадянського суспільства і демократичної держави.

Психологічні і культурологічні основи мають знайти своє відображення в праві через мовну політику, врегулювання питань пов'язаних з використанням «мови ненависті», а також побудові ефективної системи комунікації та формування публічного простору, засобів і центрів комунікації, як необхідної умови громадянського суспільства і демократичної держави.

Більш детально особливості інформаційних загроз, виникнення яких пов'язано з проведенням антитерористичної операції (гібридної війни) та повномасштабної війни проти Росії розглянуті у наступному розділі.

РОЗДІЛ 3
ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВІЙНИ

3.1. Інформаційна захищеність людини в умовах інформаційних впливів Російської Федерації

До 2014 ми не знали категорію «гібридна війна» в Україні. Поодинокі науковці вивчали і військові розуміли що це. Більше відомі були поняття «інформаційна війна/протиборство/зброя», хоча й вони використовувались в контексті майбутнього, публіцистичному стилі. Але з вказаного року ситуація змінилась. Державу окупували на сході і Криму, а по всій країні посилився вплив інформаційної пропаганди Росії.

Ще називали російсько-українську війну з 2014 року як «не конвенційна війна» (unconventional warfare), «нерегулярна війна», чи «змішана війна» (compound warfare), або ж спонсорова ні державою «гібридні війни» (State-Sponsored Hybrid). Залучаються невійськові засоби також [9]. В міністерстві оборони США науковці і посадовці окреслювали гібридну війну «як сукупність загроз з боку держав і недержавних організацій, що використовують комп'ютерні мережі та супутникові атаки; портативні ракети «поверхня-повітря»; саморобні вибухові пристрої; маніпулювання інформацією та засобами масової інформації; хімічну, біологічну, радіологічну, ядерну зброю» [116].

По суті, це новий вид агресії шляхом створення внутрішніх протиріч, конфліктів, заволодіння стратегічними ресурсами країни-жертви без оголошення війни. Фактично "compound war" ведеться в різних вимірах (інформаційному, політичному, соціальному, економічному воєнному). Звідти і випливає її назва.

Є. Магда визначає гібридну війну як прагнення однієї держави підпорядкувати собі іншу державу за допомогою економічних, політичних, інформаційних інструментів. Бойові дії є другорядними. На першому плані інформаційні операції та інші важелі впливу. Це деморалізація і залякування насамперед мільйонів людей. Завдяки швидкому поширенню інформації вона перетворилася на товар і зброю [35, с. 304].

Досвід України показує, що поле бою, на якому Росія розгорнула свої операції, є значно ширшим. Г. Почепцов зазначає, що гібридна війна розгорнута майже на всіх можливих напрямках. Це одночасно репутаційна, смислова, людська. На неї працювали всі, хто має вплив на населення: актори, письменники, режисери, співаки. Військові дії задавали фон [58]. З 24 лютого 2022 року ми ще раз засвідчимося в який раз в цьому. Але зараз ще трішки про період з 2014 року.

М. П. Требін відзначив, що під час гібридної війни важливе значення надається боротьбі за розум людей. Іншими словами, інформаційній боротьба відбувається, де основними дійовими суб'єктами виступають також цивільні (ЗМІ, ТБ, Інтернет, Ютуб, т.і.) [92, с. 113-127]. Негативні інформаційно-психологічні операції, впливи під спонсорством «рубля» закладали підґрунтя для подальших операцій, що спрямовані були проти інтересів України на всіх рівнях (особи, суспільства, держави). Була розгорнута інформаційна російська пропаганда серед населення в зоні конфлікту, поза зоною, і також серед громадян країни агресора, та серед міжнародного співтовариства.

Аналітики стверджують, що інформаційний вплив з метою підготовки до гібридної війни розпочався щонайменше в 2004 р., коли стало зрозуміло, що Україна не має наміру залишатися в фарватері російської зовнішньої політики, прагне бути самостійним суб'єктом міжнародних відносин. Тоді розпочався інформаційний вплив РФ, скерований на пропаганду і власного, і українського народів проросійськими/антиукраїнськими ідеями за рахунок підміни справжньої реальності й історичних подій, розповсюдженням

напівправди та використанням інших інформаційних технологій [28, с. 124-133].

У зовнішньополітичній сфері Росія цілеспрямовано послаблювала авторитет України на міжнародній арені. Різними шляхами створювали перешкоди євроінтеграції України, наприклад, формуючи упереджене ставлення ЄС до українською влади; поширення фейків про країну; вирощуючи агентуру, шпигунів по всіх країнах ЄС; підкуповуючи західних політиків; формуючи картинку про загниваючий «запад»; протиставляючи близькість «~~братніх~~ народів», тощо.

Поширеним явищем набула діяльність «фондів», «товариств», «аналітичних центрів», «експертів» проросійської спрямованості в Європі, а також, на жаль, каналу RT і мережі «Спутнік», які використовувались в зловісних пропагандистських цілях. Будь вони прокляті.

Внутрішня політика страждала через втручання Росії також, наприклад через підтримку політичних партій чи окремих політичних діячів, маніпулювання енергетичною залежністю, підрив авторитету владу у населення; інвестування в українські компанії, особливо в медіа; розпалювання етнічної ворожнечі; і через маніпулювання мовним питанням; нав’язування комплексу меншовартості. До речі, за даними аналітиків на 2014 рік близько 90% телекомунікаційної інфраструктури знаходилось у власності громадян РФ.

Протягом усіх років незалежності України активна інформаційно-пропагандистська робота Росії велася в Криму. Загалом, росіяни завжди насильно намагались полонити українців впродовж усіх століть нашого існування. Це досить відомо українцям, і тому детально розписувати попередні століття не будемо в цій роботі.

Країна-терорист сприяла формуванню проросійських настроїв у суспільстві, насаджуючи міф про спільний «русский мир», заперечення існування окремої від росіян української нації з власною мовою, культурою, та історією, тощо.

Науковці наводять такі основні інформаційно-психологічні методи впливу Росії, спадкоємицю школи безпеки (вбивств, точніше було б) СРСР: ЗМІ та спец. засоби пропагандистської спрямованості; глобальні комп'ютерні мережі, програмні забезпечення з пропагандою; засоби, що нелегально модифікують інформаційне середовище; чутки; генерування електромагнітних полів [1]; напівправда, фейк (симулякр) [56, с. 30-37]; дезінформування, маніпулювання, диверсифікація громадської думки, психологічний тиск, міфи, легенди [7, с. 136-141]; зниження міжнародного іміджу України задля послаблення її геополітичного значення; формування стереотипу меншовартості та вторинності українців; руйнування почуття нації та народу; домінування російської мови, культури, традицій для утвердження самоідентифікації при витісненні української мови та культури [99]; формування іміджу РФ як могутньої держави, формування уявлення про начебто підтримку сходу України дій з боку РФ; зомбування власного населення кремлівськими вигадками про американських військових, які ведуть бойові дії на сході України, про біолабораторії в Україні; підтримки проросійських громадян України [28, с. 124-133].

Дезінформація, фейки часто були продумані, правдоподібні. Була спотворена інформація, або вибірково неповна інформація, яку Росія закидала в українській інформаційний простір. Людина за наявності стійкого та міцного фільтру може приймати рішення, і діяти відповідно до адекватного змісту інформації, при цьому поведінка її буде неадекватною в реальній ситуації [99, с. 184-191].

Прикладів фейків, ІПСО, здійснених Російською Федерацією є безліч, і вони майже щоденно трапляються в інформаційних просторах.

Під час військового протистояння був створений анімаційний фільм нібито дітьми, що втекли з Донбасу в росію, основним посилом якого було «Рятуйте людей Донбасу».

На виконання вимог Роскомнадзору в соцмережі Вконтакте було заблоковано сторінки «Правого сектору» та «Євромайдану» [101].

У самопроголошених ЛНР, ДНР у 2014-14 роках заблокували доступ до українських і міжнародних ЗМК, ліквідовані місцеві проукраїнські ЗМІ, створені Міністерства інформації та зв'язку ДНР і інформаційна комісія ЛНР [93].

На окупованих територіях створюється інформаційно-пропагандистська система, яка виправдовували насильства бойовиків Росії, легітимізувала сепаратистські «уряди», дегуманізувала українську, європейську, американську нації; дискредитувала українську владу, і також деморалізувала ЗСУ [107]. Стан масової свідомості там - «фрустраційний, травмований». Свідомість – поляризована, чорно-біла, закрита для сприйняття «чужого» погляду. Мешканці там обирають ті джерела, які забезпечують психологічний комфорт. Більшість дезорієнтована, втрачає чітке розуміння добра і зла, допустимого і неприпустимого. Більшість не мають медіа-грамотності; не змогли виїхати з окупованих території, тощо.

В деяких виданнях України представили як жертву «підступного Заходу», і це ще один повторюваний мотив в дезінформації. Група хакерів КіберБеркут заявила, що має докази того, що Україна – всього лише випробувальний полігон для секретних експериментів США. Зрозуміло, жодного доказу існування біолабораторій надано не було. Це лише заява, яка неодноразово звучить з вуст пропагандистів-злочинців Кремля.

У березні 2015 року Європейська Рада доручила Верховному Представнику ЄС у співпраці з інституціями ЄС та країнами-членами ЄС представити план дій зі стратегічних комунікацій. Була створена оперативна робоча група для протидії кампанії з дезінформації з боку Росії.

Одним з прикладів діяльності комісії є спростування міфів щодо нацизму в Україні. «Значна частина дезінформації, свідками якої ми стали за останні два тижні (вересень 2017 року), зосереджена на все тій же меті – Україна. Ми побачили кілька звичайних сюжетів: «Україна – не держава», «Європа кинула Україну», «Україна позбавлена незалежності». Однак найчастіше повторюють ту стару-добру частину дезінформації, яка пов'язує

Україну з нацистами. Так, країну звинуватили в тому, що вона стала неонацистських чудовиськом, створеним Заходом, і в тому, що її окупували нацисти, які йдуть слідами Геббельса. Ніхто особливо не згадав справжню окупацію деяких районів України. Це мені нагадує ідеї, які регулярно лунають в інформаційних пропагандистських джерелах Росії.

Міністр закордонних справ Німеччини Габріель також став мішенню дезінформаційних публікацій, оскільки він привітав Україну з Днем незалежності, вживши в Твіттері вираз «Слава Україні». У цих словах швидко визнали нібито «добре відомий» нацистський слоган часів Другої світової війни, що стало ще одним прикладом винахідливого історичного ревізіонізму. Насправді вираз «Слава Україні» використовується, як мінімум, з 1919 року і знову набуло популярності після протестів на Майдані в 2013-2014 рр. В Європі досі є в 2022 році люди без критичного мислення, які були зазомбовані російськими штампами брехні, і, зокрема, про те, що патріотичне гасло «Слава Україні» - це начебто нацистський бандерівський девіз. Дуже добре, що російська пропагандистська системи Sputnik, і Russia Today - заборонені в усіх країнах ЄС. «Путін хоче не тільки захопити землю, він також хоче захопити душі людей токсичними повідомленнями, брехнею», – сказав глава європейської дипломатії Жозеп Боррель [120].

На жаль, захист інформаційного простору України розпочали навіть не відразу після початку АТО. Численні серіали, фільми, радіо, ТБ з антиукраїнськими настроями масово транслювалися в українському теле/радоефірі. Була певна невизначеність державної інформаційної політики в Україні, а також рівень фінансування.

М. Требін сказав: «Будь-яка війна колись закінчиться, а інформаційна боротьба за розум і серця людей не закінчиться ніколи» [92, с. 64-68]. Державні органи, ЗСІ повинні постійно боротися за правду, заслуговувати довіру українців, та поважати себе, і інших, простіше кажучи. Взаємодопомога, боротьба за правду, регулярна боротьба проти корупції приведе українців до процвітання, сталого розвитку.

Саме тому важливе значення має на нашу думку протидія інформаційно-психологічним операціям Росії під час воєнного стану. Так День 24 лютого 2022 р. назавжди залишиться в пам’яті українців. Це чорний день в історії України, як і подальші дні протистояння проти загарбників. Це історія, що змінила життя усього світу.

Кожен день вбиваючи українців (геноцид), держава-терорист не забуває про проведення інформаційних атак на українське населення, прагнучи за допомогою фейків посіяти в суспільстві страх та паніку, дестабілізуючи соціально-економічну та політичну ситуацію в Україні. Вторгаючись в українські інформаційний простір, ворог посягає на ідентичність громадян України.

Сучасне використання технологій, Інтернету, мобільного зв’язку окрім зручностей роблять загальну систему безпеки вразливою. Створюються передумови для витоку інформації, можливості технічного впливу на неї з метою формування потрібної суспільної думки; передачі стратегічної інформації ворогу незначними зусиллями. Реалії нецивілізованих атак російської федерації вимагають активних дій щодо забезпечення національної безпеки України.

Указом Президента України № 64/2022 тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану».

2020 року у новій редакції приймається «Стратегія національної безпеки України». Під заголовком її є «Безпека людини – безпека країни». Згідно документу, пріоритетами забезпечення національної безпеки є захист особи, суспільства, держави від правопорушення; посилення спроможностей

національної системи кібербезпеки для ефективної протидії кіберзагрозам; сприяння реалізації національних інтересів; отримання повної, достовірної інформації про ситуацію в Україні та світі; протидія зовнішнім загрозам національній безпеці України [111].

2021 року прийнята нова Стратегія інформаційної безпеки, що передбачала взаємодію на основі законів України, Стратегії кібербезпеки, Конституції України, Стратегії національної безпеки, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. Вже, нарешті, в ній конкретизуються потенційні інформаційні загрози: «інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав» [94].

Цей базовий концептуальний документ про сучасну політику України в сфері інформаційної безпеки було затверджено Указом Президента України 28 грудня 2021 р. [94]. Документ визначив 7 основних стратегічних цілей у сфері інформаційної безпеки.

У цій Стратегії дається визначення поняттю «інформаційна безпека України» як складової частини національної безпеки держави, стану захищеності державного суверенітету, демократичного конституційного ладу, територіальної цілісності, суспільства і держави, за якою належним чином забезпечуються конституційні права і свободи людини на зберігання, поширення, збирання, використання інформації, існування ефективної системи захисту та протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом; проведення терористичних актів.

У Стратегії поняття «інформаційна загроза» пояснюється як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи

ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

На думку директора Українського інституту національної пам'яті Антона Дробовича, «полем бою є не тільки терени України. В інформаційному просторі це, мабуть, найбільша медійна війна в історії людства. Це дуже публічна війна. Такого не було під час Другої світової. Навіть війна в Сирії, де Росія теж свій п'ятак вставила, не було стільки людей, які в зоні військових дій із гаджетами і Інтернетом, які це покажуть. Неймовірна кількість зафіксованих матеріалів із вебкамер, які стежать, як мародерять росіяни. Такого не було ніколи» [52].

Результатами реалізації Стратегії визначено: формування української громадянської ідентичності; захищений інформаційний простір; здійснення ефективної протидії поширенню незаконного контенту; ефективне функціонування системи стратегічних комунікацій; забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України, та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій; суттєве підвищення рівня медіа-культури та медіа-грамотності населення; дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань; захист приватного життя, забезпечення захисту прав журналістів.

В умовах війни акценти на виявлення загроз і реакцію змінились у напрямку звуження прав людини, керуючись необхідність забезпечення впливу на потенційні та існуючи загрози.

Тому, у зв'язку з веденням воєнного стану вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану» [65].

Серед конституційних норм, щодо яких можливі обмеження їх дії є і ті, що безпосередньо стосуються інформаційних прав. Зокрема:

– стаття 41 («Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності»);

– стаття 34 («Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань»);

– стаття 31 («Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції»);

– стаття 32 («Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України»).

Варто наголосити: воєнний стан не став приводом для свавільного владного трактування прав та обов'язків суб'єктів із хаотичним встановленням заборон і обмежень. Поступово, відштовхуючись від актуальності і потреб, приймаються закони, якими регламентуються правила поведінки. Ці закони стосуються врегулювання інформаційних правовідносин щодо заборони поширювати певну інформацію, враховуючи її небезпечний характер для суспільства; врегулювання моментів технічного фіксування інформації в умовах воєнного стану; встановлення чи посилення відповідальності за поширення певної інформації; врегулювання процесуальних дій щодо вилучення інформаційних даних.

Так, Верховна Рада ухвалила законопроєкт про кримінальну відповідальність за незаконну фото- та відеозйомку переміщення ЗСУ та міжнародної військової допомоги під час воєнного стану [65].

22 березня 2022 р. набув чинності Закон, яким спрощено проведення слідчих дій та тимчасових доступів до речей і документів, слідчий може здійснити фіксацію комп'ютерних даних на місці обшуку, навіть якщо про це не сказано в дозволі: зміни до КПК [64].

За виготовлення та поширення забороненої інформаційної продукції посилено кримінальну відповідальність відповідно до Закону України «Про

внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» [64].

Фейки штампуються російською пропагандистською машиною майже щодня. Приємно, що на початку грудня 2022 року у Латвії, Естонії, Литві заборонили мовлення російського ліберального каналу «Дождь». Була анульована ліцензія, яка надавала телеканалу право поширювати свій контент у країнах ЄС, США та інших країнах. 2 грудня Національна рада з електронних засобів масової інформації (NEPLP) Латвії оштрафувала телеканал «Дождь» на 10 тисяч євро за показ в ефірі мапи з окупованим Кримом у складі Росії та слова «наша армія» стосовно російської армії. Днем раніше, закликаючи глядачів ефіру писати про порушення при проведенні мобілізації та воєнні злочини, ведучий Олексій Коростельов сказав: «Ми сподіваємося, що багатьом військовослужбовцям у тому числі ми змогли допомогти, наприклад, з оснащенням і просто елементарними зручностями на фронті» [17]. Їхні рупори пропаганди під будь-якими масками слід забороняти, а після перемоги – денацифіковувати, перевиховувати росіян десятиліттями.

Компанія Google виділить 10 мільйонів доларів на боротьбу з фейками про війну Росії проти України. Про це повідомив у травні 2022 року Метью Бріттін, керівник підрозділу Google в Європі, на Близькому Сході та в Африці. Ці гроші мають піти на протидію поширенню недостовірної інформації в Україні, оскільки, каже Бріттін. Він наголошує: поширення такої інформацію в умовах війни може бути «питанням життя і смерті». За його словами, компанія вже надала 55 мільйонів доларів допомоги на підтримку України та українського народу у боротьбі проти російської агресії. Раніше Google відкрив фонд підтримки стартапів в Україні - Google for Startups Ukraine Support Fund. Компанія вирішила виділити 5 мільйонів доларів на гранти [113].

Рішенням Ради Національної безпеки і оборони від 8 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» установлено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, «ураховуючи пряму військову агресію з боку Російської Федерації, активне поширення державою-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії Російської Федерації проти України, з метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в країні правового режиму воєнного стану. В умовах воєнного стану країни дійсно особливо актуальним постало питання необхідності єдиної інформаційної політики. У зв'язку із цим Президент України підписав Указ № 152/2022, яким увів в дію Рішення Ради національної безпеки і оборони країни. Забезпечення цього рішення реалізувалось шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UAразом»«. З огляду на це рекомендовано Національній раді України з питань телебачення і радіомовлення вжити заходів щодо реалізації цього рішення [102].

Відповідно до цього Рішення декілька каналів, опозиційних до влади однак завжди з проукраїнською позицією, було відімкнуто в цифровій мережі Т2. Жоден уповноважений орган як от Національна рада України з питань телебачення і радіомовлення, Міністерство оборони України, яке відповідно до закону регулює режим воєнного стану, РНБО України чи суд не приймали рішень щодо відключення даних телеканалів [27]. Також, канал «Інтер», що був рупором російської пропаганди, майданчиком для антиукраїнських сил, став частиною проєкту «Єдині новини UAразом» [108].

Трапляються на цьому телевізійноу мовленні «Єдині новини» численні помилки. Детектор медіа повідомляє, що порушень стандартів у блоці

телеканалів ICTV та СТБ знову було рекордно багато – 273. З них 122 були «внеском» журналістів тижневика «Факти тижня», які не навчені авторизувати свої численні суб'єктивні міркування. Втім, і в новинах була завеликою кількість порушень стандарту відокремлення фактів від думок.

Порушення стандартів в ефірному блоці каналу «1+1 було загалом 105. Журналісти найчастіше порушували стандарт достовірності (45 разів). Стандарт відокремлення фактів від думок порушували 35 разів, стандарт точності – 23 рази. В блоці телеканалу «Рада» грубих порушень стандартів було 89. Найчастіше порушувалися стандарти достовірності, і відокремлення фактів від думок. По 7 разів порушували стандарти точності та повноти інформації.

У блоках каналів ICTV та СТБ, «Інтер», «1+1» однієї доби, коли був написаний цей звіт інформаційним ЗМІ «Детектор медіа», не було проявів політичного піару. Натомість, в ефірному блоці каналу «Рада» був один такий прояв – піарили заступника керівника Офісу президента Кирила Тимошенко [41].

Ми помітили також, що в телемарафоні «Єдині новини» часто піарили фамілії Єрмака (керівник ОП), М. Подоляка, К. Тимошенка. Це дає зрозуміти, що ці персони намагаються «відбілитися», і пропіаритися перед майбутніми виборами. Але, вони повинні понести відповідальність за корупційні скандали після перемоги неодмінно. М. Подоляк взагалі був радник при президенті Януковичі, і говорив повні нісенітниці, хвалив його. А, наприклад, розслідування здійснювали того, як багато Офіс Президента відмиває грошей на проектах «Велике будівництво», «Озеленення», тощо. Це досліджували вже в деяких журналістських агенціях, та це потребує втручання НАБУ, САП. Дуже прикро, що оточенні президента В. Зеленського є такі токсичні люди. Дивно, що досі він не помічає помилки, та «чорні справи» цих людей. Можливо, вони роблять це «за спиною» Зеленського. Журналісти BIHUS Info на ютуб каналі зробили розслідування щодо того, що «творить» пан Єрмак під час війни, а саме націоналізує «все,

що можна», призначає на посади своїх друзів з юридичної фірми, яку він з ними створив у 90-х роках, тощо. Це - очевидна корупція, і це засмучує українців! Детальніше про справи Єрмака дивитись за посиланням на відео-матеріал журналістів Bihus Info [50].

Варто підмітити, що майже ні разу Головнокомандувача ЗСУ Валерія Залужного не згадують в телемарафоні «Єдині новини». Інтерв'ю не роблять. Це змушує думати, що йому буцімто заборонили, аби не ставати популярнішим, і не складати конкуренцію на виборах, або мати більший вплив в інформаційному полі суспільства. Але це тільки правдоподібна теорія. Валерій Залужний і воїни України – це величезна вдача українського народу. Це подарунок. Безмежно вдячні їм..

Не можна заперечувати, що однією з цілей ворога є знищення української культури, української громадської ідентичності. Тому уряд ухвалив правильне рішення, дозволивши установам культури та мистецтв відновити роботу в умовах війни. Міністр культури та інформаційної політики Олександр Ткаченко сказав, що «діячі мистецтв готові працювати нон-стоп, аби полегшити страждання людей від пережитих жахіть війни, подарувати позитивні емоції дорослим та дітям, а також відродити надію та віру в краще майбутнє. Культура – це м'яка сила. Вона здатна повернути українців до нормального життя в новій воєнній реальності» [96]. Ми не можемо не погодитись, що на культуру необхідно виділяти багато коштів, і розвивати її. На культуру виділи в держбюджеті на 2023 рік 235 млн грн, у тому числі для забезпечення реалізації проектів Українським культурним фондом та Українським інститутом книг [6].

Українське мистецтво та культура - це імідж країни у світі. Добре, що Міністерство культури та інформаційної політики України спільно з Державним агентством України з питань мистецтв та мистецької освіти та партнерами запускають проєкт Ukraine Now and Forever. Основна мета проєкту – спрямування уваги світу до української культури і мистецтва та

подальша консолідація міжнародної спільноти у спротиві російській агресії, зокрема накладаючи більше санкцій на неї [124].

Інформаційні технології використовуються не лише в комерційній, а й у військовій галузі. Інформаційна безпека у військовій сфері є досить традиційною сферою. Захищаються від засобів розвідки як пасивними, так і активними методами. Сьогодні одним з найістотніших об'єктів безпеки в оборонній сфері є інформаційні ресурси та структура оборонного потенціалу країни. Сучасні засоби озброєння військової техніки, системи управління військами, зброєю мають високий рівень комп'ютеризації. Вони можуть бути вразливими. Дуже добре, що Україна прийняла нещодавно вітчизняну нову автоматизовану систему управління бойовими діями «Дзвін-АС» [84].

Міністр оборони повідомив про це 8 грудня 2022 року (дивитися додаток Б). 18 серпня 2022 року українцям повідомили про купівлю супутника військово призначення ICEYE та контрактний доступ до бази даних сузір'я SAR-супутників. Це сталося завдяки співпраці з БФ С. Притули. Нещодавно ГУР повідомило, що провело космічну розвідку близько 150 районів розташування ворога, як на тимчасово окупованих територіях України, так і на території окупанта та його союзників. Загалом, завдяки проекту, до якого причетні мільйони українців, виявлено та підтверджено близько 2600 одиниць військової техніки. Бойові бригади отримують потік даних з супутників ICEYE. Попередньо спеціально навчені фахівці Міноборони України розшифровують і опрацьовують свіжі данні [95].

Не даремно багато дослідників стверджують, що забезпечення військової безпеки в 21 столітті буде все більше залежати від інформаційних чинників. Американський футуролог О. Тоффлер у книзі «Війна та анти війна» [122, с. 45] зазначає, що інформація стає найважливішим військово-стратегічним ресурсом щонайменше, або навіть важливішим, ніж традиційні види озброєнь і техніки. Отже, держава, яка дає про свій оборонний потенціал, має приділяти увагу розвитку методів інформаційної протидії та

впливу. Це підтверджується історією воєн XX і початку XXI століття, у яких роль інформаційного чинника у забезпеченні оборонної безпеки різко зросла.

Доводиться визнати, що, незважаючи на значно збільшене значення інформації, інформаційних технологій у боротьби з загрозами нової епохи, сучасні агресивні країни (такі як Китай, Росія, КНДР, Іран) не мають наміру відмовлятися від військової сили як головного інструменту своєї загарбницької політики. Простіше кажучи, добро повинно мати кулак.

Держава вимушена була впровадити обмеження, бо інакше неможливо було б захистити осіб на території України від свавілля ворога. До того ж, Україна не може нести відповідальність за порушення цих прав на непідконтрольних, внаслідок окупації, територіях та місцях ведення бойових дій. Інше їх значення полягає у можливості прийняття нормативно-правових актів, спрямованих на захист інформаційної безпеки держави. Такі пріоритети можуть йти в розріз з правами людини, однак в час війни перевага інтересів держави означає можливість збереження основоположних прав багатьох людей через забезпечення життєдіяльності самої держави. Завершення воєнного стану автоматично активує тимчасово призупинену дію вищеназваних норм. Строк воєнного стану та проведення загальної мобілізації продовжується з 21 листопада 2022 року на 90 діб [104].

Сподіваємося, помилок в телемарафоні «Єдине мовлення», корупційних випадків буде ставати менше в Україна. Необхідно, щоб створили відповідні штрафи, та понесення відповідальності усіх посадовців, які вчиняються корупційні дії в період воєнного стану. Детальніше про інформаційні скандали та комунікацію уряду буде в наступному підрозділі.

В Україні за повномасштабну війну волонтерський рух став безпрецедентний. Скільки автівок, дронів, броні завдяки волонтерам на фронті, байрактари, супутник, бпла, та купа іншого - таке було тільки в Україні. Це вже не просто рух, це історія, а далі ще більше. 5 грудня в Україні відзначали день волонтера. Сумно, коли був якийсь певний момент в медіа, коли волонтерів цькували без причини, робили купу репортажів,

шуму, критикували безпідставно фонд того ж С. Притули, начебто відводячи увагу від помилок Офісу Президента. Але ця ситуація вже владналась. Восени, взимку 2022 року вже такого не спостерігаю.

Прикро, що не понесли досі відповідальність голова Дніпровської області Резніченко, який перевів півтори мільярди гривень для ремонту доріг на рахунки фірми своєї подруги, тренері по армреслінгу [3].

Не понесла відповідальність досі запорізька адміністрація за розкрадання гуманітарки в Запоріжжі. Національне антикорупційне бюро (НАБУ) під час одного з обшуків у кримінальному провадженні за фактом імовірного розкрадання гуманітарної допомоги в Запорізькій області вилучили понад 230 тисяч доларів та понад півмільйона гривень готівки. Це був гучний скандал вересня 2022 року [10].

В жовтні екс-нардепа і забудовника Максима Микитася затримали після спроби дати багатомільйонний хабар міському голові Дніпра Борису Філатову. Про це 18 жовтня повідомила прес-служба НАБУ. Слідство повідомляє, що колишній народний депутат України Максим Микитась запропонував міському голові Дніпра Борису Філатову хабар за укладення з підконтрольними йому компаніями контракту з будівництва метрополітену в Дніпрі поза конкурсом. Кошти обіцяв надавати частинами впродовж дії проекту – до 2027 року. «Лояльність» мера екс-нардеп оцінив у 10% від вартості проекту (220 млн євро), що становить відповідно 22 млн євро [37].

Український журналіст Юрій Бутусов написав текст, який є досить правдоподібним і змушує задуматись щодо «друзів», посадовців ОП, які не понесли відповідальність за свої помилки, злочини. Текст такий: "Страшна ціна брехні президента Зеленського на скандальній прес-конференції: тепер кожен розуміє, чому я поставив президенту питання про Демченка. Рік тому, 26 листопада відбулась відома прес-конференція, на якій я задав питання президенту Зеленському, чому він незаконно, в порушення закону про люстрацію, призначив на найвищий пост - начальника Комітету по розвідці при президенті України російського агента Руслана Демченко. На питання

Зеленський не відповів, не пояснив чому він порушив закон, натомість почав захищати Демченка, який на цій посаді відповідав за розвідку проти Росії, і попередження держави та населення. Цікава деталь, яку кожен може перевірити - у російських ЗМІ ніяких критичних згадок щодо Демченка ні до після тієї прес-конференції не було взагалі, бо він для них - свій. Моє питання, яке залишилось без відповіді, зараз показує чому не було проведено розгортання територіальної оборони; не було негайно підірвано мости через Чонгар, мости через Дніпро у Херсоні; не були прикриті тили гарнізону Маріуполя, здані без бою Мелітополь, Бердянськ, тобто росіянам відкрили "коридор у Крим"; не було проведено мобілізацію оперативного резерву; не встановили загородження на шляхах російського наступу (та інші питання). Ось чому Зеленський продовжував брехати про «шашлики на травневі свята».

А багатомісячні попередження про напад з боку країн НАТО Зеленський та його Слуги називали провокаціями і замість мобілізації брехали людям щоб не дати можливості багатьом діяти самостійно. Після початку війни Р. Демченко виявився непотрібним, бо начальник комітету по розвідці України Демченко не користувався довірою країн НАТО, з ним не хотів спілкуватись жоден західний розвідник. Тому він одразу виявився відстороненим, формально його відсторонили від посади у червні, але Демченко залишався ще до кінця серпня на посаді у комісії по громадянству при президенті України. Зеленський і зараз продовжує тримати біля себе начальника розвідки, який "прогавив" російський напад і підставив Україну, він не сидить у СІЗО, йому не пред'явили звинувачень, нема його і на фронті. Проти Демченка нема зараз ніяких розслідувань, президент робить вигляд, ніби російський напад був несподіваним. Дуже цинічно, що В.Зеленський звинуватив мене на прес-конференції, ніби якісь українські військові загинули через мої дописи. Хто саме, жодних імен він не назвав, ніяких розслідувань, ніяких фактів не представив. Маємо надію, що будуть проведені детальні розслідування журналістами та відповідними органами

щодо безладу, корупції в оточенні президента Зеленського. Українське суспільство має почути правду та відповіді. Українці мають багато запитань до влади. І сподіваємось, що зазначені персони точно постануть перед судом, хоча б, після перемоги проти російської нечисті.

Якщо зазначені лише ці декілька персон зверху не будуть нести покарання, то у суспільства буде падати довіра до уряду. Як кажуть, «не так страшні чужі гниди, як наші воші». Але українське суспільство є об'єднаним, сильним, як ніколи, і ми обов'язково розберемося з зовнішнім, і внутрішнім злом. Будемо сміливо боротися, допомагати один одному, і поступово станемо кращими.

Хочу звернути також увагу на певну вибірковість наших ЗМІ, що не може не обурювати. Наприклад, співак Монатік віддав 100 000 грн. з свого концерту на ЗСУ, і численні медіа про це написали. Тим часом, весь час повномасштабної війні названі мною Youtube-канали збирають мільйони гривень для ЗСУ, а телебачення, ЗМІ, натомість, майже не згадують про них [110].

Нові інформаційні технології відкрили нові можливості отримання інформації про противника, попередження про можливі конфлікти та напади. Прикро, що український уряд отримував повідомлення від США, В.Б. про можливий напад РФ, але не вірив цьому, не інформував населення про хід дій у разі нападу, а, натомість, заспокоював, і т.і. Це не правильно. Говорити правду – необхідно. Наголошую ще раз, що її треба вміти говорити. А суспільство не панікувати і діяти раціонально, з холодним розумом, розумінням. Ще прикро, що не була продумана оборона Маріуполя, Херсону. Не були підірвані мости. Начальник штабу полку «Азов» Богдан Кротевич розповідав в інтерв'ю після звільнення з полону, що обов'язково після перемоги займеться розслідуванням щодо тих генералів, чиновників, прокурорів, мерів, які здали оборону Херсону, Маріуполя, прирікши тисячі українських життів на смерть від підступного ворога. Генерали, навіть, не

зробили план оборони цих міст [43]. Наразі за деокупацію наших територій українці платять кров'ю та здоров'ям.

Національний центр Олександра Довженка «Довженко центр» хотіли у листопаді 2022 року безпідставно і незаконно ліквідувати певні «злі персони» з Офісу Президента, Держкіно, керуючись власними інтересами. Українське суспільство було обурене і вийшло на протести. Поки що зупинили цей процес Комітет гуманітарної та інформаційної політики на черговому засіданні, що відбулося 15 листопада, вдруге розглянув питання реорганізації «Довженко-Центру» й ситуацію, яка склалася після цього скандального наказу Держкіно. Народних депутатів стривожили акції протесту біля «Довженко-Центру». Раніше комітет уже рекомендував керівництву Держкіно скасувати наказ про реорганізацію «Довженко-Центру». За кілька годин після засідання комітету Державне агентство з питань кіно повідомило, що призупиняє дію наказу про реорганізацію «Національного центру Олександра Довженка» до завершення повного аудиту й обрання нового керівника.

Ось так Держкіно скоріше через якісь мрії корупційних схем разом з депутатами, з ОП, хотіли ліквідувати конкурента. Державне агентство України з питань кіно опубліковало наказ, що тимчасово обов'язки керівниці Довженко-Центру виконуватиме Каждан Юлія Романівна, яку на сайті установи називають професійним кризовим менеджером. У ЗМІ з'явилась інформація, що Юлія Каждан керує кінологічним центром та не має досвіду роботи у сфері кіно, що викликало обурення та кепкування у соцмережах. Також, вона займається гіпнозами. Ми вважаємо, що на будь-яких посадах не повинні бути не компетентні, не кваліфіковані люди. Це знущання над українцями, знищення розвитку культури [11].

Ці питання обов'язково владнаються. І сподіваємось, щоб було більше проектів, заходів, що забезпечить стабільний розвиток культури. Культурна експансія України була б не зайвою. Світ має чути про Україну ще й в цій сфері. Ми маємо купу талановитих акторів, про які, на жаль, мало чуємо

наразі. Громадянам слід ознайомлюватись з їх творчістю. Слід споживати український контент у всіх сферах. Якщо не будемо споживати, розвивати, то й світ не буде зацікавлений.

Цивілізований світ – на боці України. Кремлю уперше за багато років програв начисто світове інформаційне поле. До речі, Росія створювала фейки, що Зеленський буцімто вже в США, що він покинув народ. Однак, президент Зеленський, міністерства, та інші відомства, більшість депутатів – великі молодці, що не покинули посади, коли Росія розпочала повномасштабне вторгнення. І, авжеж, велика дяка збройним силам, що дала перший відсіч навалі ворога. Битва по всіх фронтах досі триває. Уряд і прекрасні українці борються. Допомога від західних партнерів надходить щонеділі. Нові списки допомоги різного роду оголошуються регулярно. Головне, аби військова допомога збільшувалась, хоча нам ніхто нічого не винен, і аби здоров'я воїнів міцнішало. Пам'ятаємо, якою ціною! Це зло буде обов'язково переможено і території будуть звільнені.

Підводячи підсумок, інформаційна стійкість необхідна в Україні. Ми знаходимося поряд з небезпечним сусідом. Тому, медіа-грамотність населення, ефективна комунікація уряду з суспільством та інші інструменти протидії неправдивій інформації мають місце бути.

Дуже хочеться нам сподіватися, що всі ці корупційні чиновники, депутати, такі як Трухін, що намагався дати хабар поліцейському в розмірі 150 тисяч доларів, та інші політичні діячі, бізнесмени будуть нести справедливу відповідальність та покарання. Побажаємо САП, НАБУ, та Вищому Антикорупційному суду України сил, незалежності, і ще раз сил.

Тому, держава має вести ефективну інформаційну діяльність для мирного врегулювання кризових ситуацій. У разі ігнорування можуть виникати радикальні настрої, спалахи ворожості, які спричинені ззовні, або зсередини. Військові, застосовуючи інформаційні технології, відкрили нові можливості щодо забезпечення оборони держави, звільнення окупованих територій. Поряд з озброєнням, боєприпасами, транспортом, інформація

посідає важливе місце. Виграші у інформаційному протиборстві під час війни з Росією сприяє досягненню стратегічних цілей.

У Стратегії інформаційної безпеки України 2021 року відображено інтереси держави, які виражаються у необхідності ефективного захисту конституційного устрою суверенітету та територіальної цілісності країни, встановлення та підтримання політичної стабільності, включаючи стабільність державної влади та її інститутів. Аналіз ходу реалізації цілей Стратегії показав, що цей процес не зупиняється, незважаючи на всі труднощі воєнного стану.

3.2. Рекомендації щодо безпеки для громадянина в інформаційному просторі піл час воєнного стану

Зважаючи на шалений потік інформації під час війни, вважаємо, що суспільство повинно мати хоча-б якийсь рівень медіа-культури, медіа-грамотності. За 9 місяців війни українці вже точно «набили руку» і одразу вичислюють російський слід в інформаційній умовній одиниці. Більшість є обізнаними. Хоча ніхто не застрахований і ми повинні перевіряти джерела, бо можна випадково «повестись» на неправдиву інформацію. В такому шаленому потоці інформації це може трапитись, що є нормальним. Для найпростішого нівелювання ризику – підписатись на офіційні джерела України.

Рекомендують підписатись на перевірені українські Telegram-канали, яким довіряєте. Додаток Telegram є дуже популярним серед українців наразі. Завдяки ньому ми отримуємо інформацію, навіть, швидше, ніж з телевізора. Російська Федерація і тут вклали великі гроші, створивши купу пропагандистських каналів, ботів, щоб робити дестабілізацію у суспільстві.

Приклади проросійських телеграм-каналів дивитись в додатку (додаток А). Ми радимо підписатись на декілька популярних українських Telegram-каналів. На платформі є також канали офіційних джерел України. Але перевіряйте їх перед підпискою. Не варто підписуватися на жодне російське новинне джерело. Навіть, якщо росіянин є автором умовного джерела, в якому хвалить, підтримує українців – то все-одно уникайте, блокуйте, не підписуйтесь на це джерело. Тому що росіяни насамперед думають про свою країну, своє благополуччя, а не про українців. Не шукайте хороших росіян. Більш того, Росія спонсорує російських авторів цифрового контенту, які втираються в довіру українців, а потім підкидують фейки поміж своїх промов, різноманітні ІПСО (інформаційно-психологічні операції), тощо. Не буду називати приклади цих негідників, бо вони не заслуговують нашої уваги. Вони повинні бути у в'язниці.

Так, зауважимо, що люди мусять удосконалювати навички медіа-грамотності, щоб не панікувати до того, як перевірять інформацію. Щоб відрізняти брехню від правди, виявляти ботів у соціальних мережах. І необхідно підключати українців до української мережі, і блокувати російські джерела, аби хтось з українців випадково не знаючи слухав регулярно неправдиву інформацію, самому цього не усвідомлюючи. Це може бути бабуся, дідусь в якомусь селі, де ловить російське брехливе телемовлення.

Не можна також фіксувати переміщення ЗСУ. Не можна фотографу ти одразу прильоти ракет ворога. Це є очевидно, але є важливою рекомендацією під час воєнного стану. Є закон «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану».

Є на Youtube платформі ряд гумористів, стендап-коміків, активістів, що роблять різноманітні розважальні заходи в містах України, і збирають кошти на ЗСУ. Вони щонеділі збирають сотні тисяч гривень. Вони – неймовірні молодці. Наведу декілька назв Youtube-каналів, які займаються подібними благородними заходами, і виробництвом україномовного культурно-значимого контенту, який відіграє значну ролю в війні про ворога. Це Youtube-канали: «hromadske», «Точка збору», «Ярема Дух», «Підпільний Стендап», «Stand-up Battle Club», «BIHUS info» «ЧерепаХа», «Останній Капіталіст», «Історія Без Міфів», «OLDboi» «ПОПЛАВА», «Militarnyi», «Клятий раціоналіст», «Розмова», «Rozetka», «Падон», «Загін кіноманів», «Dima Maleev», «Geek journal", «Aleksey Durnev», «Keddr.com», «Телебачення Торонто», «Андрій Шараєвський», «Blogmayster", тощо. І це ми не усіх згадали! Можна знайти на згаданій платформі українських авторів на різну тематику. Вони здійснюють неабиякий позитивний інформаційний вплив на мільйони українців. Українці масово відписуються від російських Youtube-авторів цифрового контенту, і дивляться вітчизняних авторів. На жаль, є ще українці, які дивлять контент росіян в Youtube, та інших платформах, що є досить сумно, але, сподіваюсь, їх стане менше з часом.

Завдання реінтеграції громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територій, до загальноукраїнського інформаційного простору було і є поки досить складним під час повномасштабного нападу Росії на Україну. Тим більше в період воєнного стану воно є ще складнішим. Тимчасово окупованих територій побільшало, і ворог робить все, щоб розірвати інформаційні та культурні зв'язки українців з Україною, які там проживають. Наприклад, знищують телевежі, захоплюють їх, включають російські каналі. Навіть, в селі Миколаївської області, в якому автор дипломної роботи зараз знаходиться як ВПО, помітив, що у деяких селян є по телебаченню російські канали. Якихось не медіа-грамотних переважно престарілих людей Росія точно вдається зомбувати. Телеканали (загалом, ЗМІ) є особливо ефективним

засобом формування української громадянської ідентичності. Тому цьому питанню треба буде приділити особливу увагу одразу після перемоги. України. Також велика роль у вирішенні цієї проблеми має бути відведена гуманітарній освіті.

Аналітики справедливо вказують на те, що «інформаційна стратегія не може існувати окремо від комплексної державної стратегії реінтеграції. По суті, інформаційна стратегія – це складова частина загальної стратегії. Одне з головних завдань ЗМІ – просування через інформаційний простір державної стратегії реінтеграції: донесення проєкту спільного майбутнього з чітко визначеними параметрами життя у об'єднаній країні; її роз'яснення і громадське обговорення; реалізація через інформаційний простір просвітницьких, освітніх, ціннісно-формуючих завдань» [83].

Також, ефективна комунікація є передумовою становлення демократичного суспільства. Особливого значення вона набуває у багатонаціональних державах, де культура спілкування відрізняється не лише на мікрорівні (особистість, група), а й на макрорівні (історичний досвід, віросповідання, регіони). Соціокультурна ситуація визначає наскільки ефективним буде комунікативний процес в суспільстві, наприклад між органами влади та населенням, між центральними органами влади, місцевим самоврядуванням та органами самоорганізації населення, між містом та селом, а також між різними регіонами держави. Від цього залежить, які саме загрози інформаційно-психологічній безпеці людини і суспільства можуть актуалізуватись.

У Доктрині НАТО наводиться визначення стратегічних комунікацій. Це скоординоване і належне використання комунікативних можливостей НАТО, а саме публічної дипломатії, зв'язків з громадськістю, PR-служби збройних сил, інформаційних і психологічних операцій для підтримки політики Альянсу і заходів, спрямованих на просування цілей НАТО [22]. Тому, стратегічна комунікація – це внутрішня і зовнішня комунікація. Зв'язки з громадськістю – один з складників стратегічних комунікацій.

Ми вважаємо, що органи державної влади, місцевого самоврядування демонструють високий рівень інформаційної взаємодії з суспільством в умовах війни. Міністерства та відомства, мери систематично доводять до суспільства актуальну інформацію, наприклад, через соц.. мережі, дублюючи інформацію на офіційних сайтах. Виступи Президента України, голів обласних військових адміністрацій, присвячені аналізу поточної ситуації, звіту про свою роботу, стали для громадян звичними. Важливо, щоб уряд, публічні особи, чиновники вчилися не заспокоювати, а говорити правду, розповідати сухі факти, ситуацію, яка є. А українцям слід не панікувати, а, натомість, діяти з холодним розумом, тому що паніка в суспільстві грає на руку ворогу. Тому нехай влада вчиться говорити правду правильним чином.

Підсумовуючи цей розділ, варто зауважити, що захист інформаційного простору України розпочали не відразу після початку АТО. Численні серіали, фільми, радіо, ТБ з антиукраїнськими настроями масово транслювалися в українському інформаційному просторі. Була певна невизначеність державної інформаційної політики в Україні, а також рівень фінансування.

Війна проти пропагандистською машини крові відбувається на всіх фронтах. Чудово, що в боротьба нам допомагають держави Заходу, зокрема в інформаційному протиборстві, хоча вони не винні нам нічого. Блокуючу рупори пропаганди Росії в ЄС та США лише роблять користь всьому світу.

Зовнішні комунікації мають працювати на формування позитивного іміджу України, як внутрішнього, так і зовнішнього. Це необхідно, щоб мати вплив на політичну, економічну, культурну перспективу розвитку країни. Особлива роль у іміджевій політиці належить органам влади, які відповідають за зв'язки з громадськістю, ЗМІ, та іншими структурам суспільства. А в умовах воєнного стану імідж формувати можна і треба.

Держава вимушена була впровадити обмеження, бо інакше неможливо було б захистити осіб на території України від свавілля ворога.

Впершу чергу треба розвивати військову силу, незважаючи на значно збільшене значення інформації, інформаційних технологій у боротьби з

загрозами нової епохо. Сучасні агресивні країни не мають наміру відмовлятися від військової сили як інструменту своєї загарбницької політики.

САП, НАБУ, Вищий Антикорупційний суд України сил повинні й надалі незалежно працювати під час воєнного стану з метою контролю, ловлею корупціонерів.

І на останок, повторимо, що необхідно завжди критично підходити до оцінки інформації, а особливо у випадках, коли джерело є невідомо, заголовок є явно маніпулятивним, зміст містить оціночні судження, емоційні забарвлення, або коли відсутнє посилання на офіційне джерело інформації. «Будь-яка війна колись закінчиться, а інформаційна боротьба за розум і серця людей не закінчиться ніколи»

ВИСНОВКИ

У цій роботі було розглянуто інформаційну безпеку України з 1991-2022 рр. Була охарактеризовано її законодавство в цій сфері з моменту створення та під час воєнного стану. Історії формування правового регулювання інформаційної безпеки України було виділено цілий другий розділ дипломної роботи, і законодавство з інформаційної безпеки 2021-2022 років детальніше висвітлено в четвертому розділі. Задля розуміння поняття «інформаційна безпека» було виділено перший розділ. У цьому розділі ми розглянули тлумачення поняття «інформаційна безпека» та проаналізували започаткування та розвиток системи національної безпеки країни.

Основною метою роботи є дослідження інформаційної безпеки України, її становлення, та стан захищеності під час гібридної війни, і в період військового стану. Систему інформаційної безпеки України розвивалася, очевидно, безсистемно, ситуативно, і під впливом різних моделей правового регулювання інформаційної сфери. Не можна повністю копіювати систему безпеки інших країн, не враховуючи особливості української законодавства, геополітичного розташування, історії, політики, правової системи. Як раз у другому розділі було розглянуто правове регулювання, основні документи, закони в сфері інформаційної безпеки, створені з дня незалежності по 2015 рік. Була можливість провести аналіз та порівняти Стратегії та Доктрини з інформаційної безпеки різних періодів, їх редакції, вплив на законотворчі процеси досліджуваної сфери. Було вказано перешкоди, помилки уряду, що перешкоджали ефективній реалізації законів та інших документів щодо інформаційної безпеки.

Аналіз становлення законодавства у інформаційній сфері в цілому та інформаційної безпеки дозволило зробити висновок, що інформаційна законодавство та законодавство щодо інформаційної безпеки є відносно новою галуззю законодавства України і все ще знаходиться на етапі

становлення, а під час воєнного стану урядом країни приймають поступово важливі закони, які дозволять підвищити міць безпеки в усіх сферах, і врятувати стабільність та демократичний фундамент в державі. Більш того, у другому розділі було згадано про основну загрозу, Росію, та наведено приклади їх інформаційних пропагандистських впливів, та протидії уряду, ЗМІ, громадянського суспільства, міжнародних компанії. Подібні приклади будуть траплятися майже в кожному наступному розділі задля більшого розуміння загроз, які постали перед Україною, яка геополітично має не просте розташування.

Стан українського законодавства у інформаційній сфері свідчить про його невпорядкованість, неузгодженість та безсистемність. Розробка законодавства щодо інформаційної безпеки людини вимагає створення ефективних механізмів активної участі у законотворчій діяльності її суб'єктів – належний доступ до проектів нормативних актів у цих сферах, реальні публічні обговорення, а також врахування їх результатів. Оскільки ця сфера відносно нова, надзвичайно динамічна і наукоємна, то й вимагає використання наукового потенціалу при розробці законопроектів у цій сфері, а також проведення експертного оцінювання ефективності вже існуючого законодавства.

Також ми приділили увагу стану кібербезпеки в Україні, зокрема її правового забезпечення, прикладів, та підкреслили необхідність її розвитку. Сучасні реалії війни показали необхідність покращення всіх сфер інформаційної безпеки.

Виокремлюють наступні етапи його становлення: I. 1992 -1996 роки – становлення основ інформаційного законодавства; II. 1996-2003 роки – усвідомлення і формулювання основ інформаційної безпеки як складової національної безпеки; III. 2003-2014 роки – усвідомлення розвитку глобального інформаційного суспільства, приєднання до міжнародних актів щодо у сфері інформаційного суспільства, права і безпеки, розвиток національного законодавства згідно з тенденціями міжнародного права; IV.

2014 – донині – розвиток законодавства у сфері інформаційної безпеки, спрямований на посилення позицій України у гібридній війні; V. 2022 – донині – розвиток законодавства і розробка законів вже під час воєнного стану.

Ми навели загальна класифікацію загроз, що може очікувати громадянина, і також розглянули стан безпеки в інформаційному просторі. В третьому розділі приділили увагу небезпекам для дітей в мережі Інтернет, та особливості правого забезпечення окремим категорій осіб населення. Різні категорії осіб знаходяться у неоднакових умовах щодо можливості реалізації своїх прав і свобод в інформаційній сфері що визначає їх ступінь захищеності в інформаційному суспільстві, види і інтенсивність небезпек, що їм загрожують.

Слід звернути увагу, що проблеми захисту від інформації суттєво складніші за проблеми захисту інформації, оскільки загрози, що виникають внаслідок інформаційних впливів надзвичайно різноманітні, їх вплив не завжди очевидний, а відвернення цих загроз або їх нейтралізація вимагають різноманітних неординарних дій. Інформаційні загрози є складним ієрархічним утворенням з множиною різнорівневих зв’язків, їх вплив на людину комплексний і різноманітний, а з позицій психологічної науки результат впливу завжди психологічний, навіть якщо за змістом він є фізичний, хімічний чи соціальний. Таким чином, інформаційний вплив завжди визначає поведінку людини прямо чи опосередковано, через психічні механізми головного мозку. Доктриною інформаційної безпеки України захищеність від руйнівних інформаційно-психологічних впливів визначено як життєво важливі інтереси особи в інформаційній сфері України. До того ж, в роботі зазначено про небезпеку використання додатків, браузерів, пошукових сервісів російського виробництва, такі як Vkontakte, Jandex, Odnoklasniki, тощо.

Ми проаналізували помилки уряду в інформаційній політиці після нападу Росії з 2014 року та дійшли до висновку, що інформаційна протидія з

початком АТО почалася пізно. По телебаченню показували російські серіали, фільми. Інші приклади інформаційної боротьби, або помилок, бездіяльності наведено в цьому розділі, яку дають загальну картину діяльності уряду та інших структур в боротьби проти загарбницької політики держави-спонсора тероризму Росії. ї

Перечислити декілька інформаційних скандалів, що відбулися під час воєнного стану 2022 р.. Особливо, коли після подібних корупційних злочинів українське суспільство не бачить суду над відповідними особами, то довіра і обурення наростає. Дані проблеми зазвичай врегульовуються ефективною комунікацією уряду, але українському суспільство необхідна буде правда, справедливість, хоча б після закінчення активної фази війни проти великого зла під назвою «росіяни». Інакше, це призведе до протестів, дестабілізації, та зміни влади на більш відповідальний уряд, налаштований виправдовувати надії народу, та нести відповідальність за свої вчинки. Тим часом, армія буде розвиватися незалежно від політичної обстановки.

Ми дійшли до висновку, що ефективна інформаційна діяльність може суттєво поліпшити зусилля держави щодо мирного вирішення кризових ситуацій. У разі ігнорування інформаційних чинників, можуть виникати найрадикальніші настрої, спалахи ворожості, що призведе до внутрішньої дестабілізації, що буде «грати на руку» ворогу українців.

В роботі обґрунтовано необхідність інформаційної безпеки в військовій сфері, впровадження новітніх технологій, що дозволить збирати інформацію про ворога швидше і якісніше. Застосування інформаційних технологій військовими відкрило нові можливості щодо забезпечення оборони держави. Володіння інформаційними ресурсами та його захист у військовій сфері стали таким самим неодмінним атрибутом, як озброєння, боєприпаси, транспорт, тощо. Виграш України в інформаційному протиборстві під час війни з Росією сприятиме досягненню її стратегічних цілей.

Інформація є зброєю «масового ураження». Відповідно, необхідно створити ефективний механізм, який би забезпечив державну інформаційну

безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію. Найбільша цінність українців полягає у їх розумінні та сприйнятті понять свобода і справедливість. Саме це вони зараз відстоюють, і розплачуються за них власним життям.

Формування інформаційної безпеки в умовах війни є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства. Варто зауважити, що за умов воєнних дій держава часто об’єктивно неспроможна гарантувати права людини в повному об’ємі. Однак, збереження фундаментальних засад на основі політичної та правової взаємодії механізмів забезпечення інформаційної безпеки оберігає підвалини демократії та систему загальних принципів права від руйнування.

Отже одним з головних джерелом добробуту людини стає інформація, то інформаційна безпека людини має на меті забезпечення збереження цілісності особи та її здатності до розвитку як визначальних категорій буття людини, враховуючи реалії становлення інформаційного суспільства.

Смерть окупантам, і сил українським воїнам. Вічна слава полеглим за Україну. Нехай спочивають в мирі. Не пробачимо ніколи, помстимося, і пам’ятатимемо.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Алещенко В.І., Сербін В.Г. Проблеми захисту від негативного інформаційнопсихологічного впливу противника. Мат. машини і системи. 2010. № 1. С. 77-86.

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

3. Близька подруга голови Дніпропетровщини отримала 1,5 мільярда на дороги в області. URL: https://www.epravda.com.ua/news/2022/11/2/693358/.

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

5. Більше половини жителів сіл в Україні вже користуються інтернетом URL:http:// watcher.com.ua/2017/04/13/bilshe-polovyny-zhyteliv-sil-v-ukrayini-vzhekorystuyutsya-internetom/ (дата звернення: 04.10.2017)]. Зведені дані, опубліковані аналітичною ініціативою DataReportal у січні 2021 року, показали, що при загальній чисельності населення 43,6 мільйона в Україні є 29,47 мільйона індивідуальних користувачів Інтернету, що становить 67,6 відсотка проникнення [Freedom House. Ukraine URL: https://freedomhouse.org/country/ukraine/freedom-net/2021.

6. Верховна Рада України ухвалила держбюджет на 2023 рік. ULR: https://www.kmu.gov.ua/news/verhovna-rada-ukrayini-uhvalila-derzhbyudzhet-na-2023-rik.

7. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентові України. 2015. № 1. С. 136-141.

8. Глобальний звіт про розвиток інформаційних технологій-2015 URL: http:// edclub.com.ua/analityka/riven-rozvytku-informaciyno-komunikaciynyh-tehnologiyv-ukrayini-ta-sviti (дата звернення: 24.09.2016).

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

10. Гучний скандал з розкраданням гуманітарки у Запоріжжі: все, що відомо на сьогодні. URL: https://zanoza-news.com/a/2022/09/13/36091.

11. Гіпноз, Собаки І Бухгалтерія: Нова Очільниця Довженко-Центру Не Має Жодного Стосунку До Кіноіндустрії. URL: https://www.slidstvo.info/articles/gipnoz-sobaky-i-buhgalteriya-nova-ochilnyczya-dovzhenko-czentru-ne-maye-zhodnogo-stosunku-do-kinoindustriyi

12. Довгань О. Д. Теоретико-правові основи забезпечення інформаційної безпеки України: автореферат... д-ра юрид. наук, спец.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право / Ін-т законодавства ВР України. К., 2016. 44 с.

13. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009. URL://www.president.gov.ua/documents/9570.html.

14. Доктрина інформаційної безпеки України, затв. Указом Президента України від 25 лютого 2017 року № 47/2017 URL: http://www.president.gov.ua/ documents/472017-21374.

15. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядноправові аспекти: Моногр. Х.: Майдан, 2011. 244 с.

16. Еріксен Т.Г. Тиранія моменту. Швидкий і повільний час в інформаційну добу / пер. з англ. В. Дмитрука. Л.: Кальварія, 2004. 30 с.

17. Естонія слідом за Латвією та Литвою припиняє мовлення «Дождя» URL: https://www.radiosvoboda.org/a/news-dozhd-estoniya-zakryttia/32167484.html.

18. Етимологічний словник української мови : у 7 т. Т. 1. К.: Наукова думка. 1982. 632 с.

19. Золотар О.О. Віртуальна реальність. Моделі колективної безпеки: інформаційний вимір: Зб. мат. / Упоряди. Ланде Д.В. К.: НДЦПІ НАПрН України, 2011. С. 63-66

20. Золотар О.О. Правова охорона як складова інформаційної безпеки: моногр. – Київ: ТОВ «ПанТот». 2011. 100 с.

21. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. Правова інформатика. 2009. № 4(24).

22. Картки: що таке стратегічна комунікація і кому вона потрібна. URL: https://cpc.com.ua/ articles/kartki-scho-take-strategichna-komunikaciya-ikomu-vona-potribna.

23. Кафтя А.А. Інформаційне законодавство України: стан та тенденції розвитку URL: http://goal-int.org/informacijne-zakonodavstvo-ukraini-stan-ta-tendenciirozvitku/ (дата звернення: 21.05.2016).

24. Кібер-буллінґ: небезпечне віртуальне «бикування» URL: http://osvita.
mediasapiens.ua/mediaprosvita/research/kiberbullin_nebezpechne_virtualne_
bikuvannya/ (дата звернення: 09.10.2017).

25. Кравець Є. А. Інформаційна безпека держави. Юридична енциклопедія: в 6 т. К.: Укр. енцикл., 1992. С. 744.

26. Красноступ Г.М. Організаційно-правові аспекти необхідності реформування сучасного інформаційного законодавства. Право України. 2005. № 9. С. с.82

27. Концерн РРТ вимкнув мовлення «Еспресо» в цифровій мережі Т2: відкритий лист телеканалу до президента, РНБО, СБУ, Міноборони, Нацради. Еспресо. URL: https://espreso.tv/kontsern-rrt-vimknuv-movlennyaespreso-v-tsifroviy-merezhi-t2-vidkritiy-list-telekanalu-do-prezidenta-rnbo-sbu-minoboroni-natsradi (дата звернення 20.04.2022).

28. Лазоренко О.А. Інформаційний складник гібридної війни Російської Федерації проти України: тенденції розвитку. Стратегічні пріоритети. 2015. № 3. С. 124-133.

29. Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України : дис. … канд. юрид. наук : 12.00.01/ Київський нац. ун-т внутр. справ. К., 2002. с.66

30. Левченко О.В. Проблеми і шляхи формування системи інформаційної безпеки держави. Зб. наук. праць Харків. ун-ту Повітряних Сил. 2014. Вип. 2(39). С. 166-168.

31. Литовченко І. Діти в Інтернеті: як навчити безпеці у віртуальному світі: посібник для батьків / І. Литовченко, С. Максименко, С. Болтівець та ін. К.: Вид. будинок «Аванпост-Прим», 2010. 48 с.

32. Ліпкан В.А. Національна безпека України: навч. посіб. К.: КНТ, 2009. 576 с

33. Логінов О.В. Гносеологічний аспект управління інформаційною безпекою України . Наук. вісн. Юридичної академії МВС України. 2004. № 2. С. 153-161.

34. Лоренц К. Агресія (так зване «зло») URL: http://lib.ru/PSIHO/LORENC/ agressiya.txt (дата звернення: 19.10.2017).

35. Магда Є.В. Гібридна війна: вижити і перемогти. Х.: Віват, 2015. 304с.

36. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис... канд. юрид. наук: 12.00.01 / Київ. нац. ун-т внутр. справ. Київ, 2007. 20 с

37. Максима Микитася спіймали на спробі дати хабар меру Дніпра. URL: https://zaxid.net/eks_nardepa_maksima_mikitasya_spiymali_na_sprobi_dati_habar_meru_dnipra_n1551379.

38. Малик Я.Й. Інформаційна безпека України: стан та перспективи розвитку. Ефективність державного управління: Зб. наук. праць. 2015. Вип. 44. С. 13-20.

39. Марценюк О.Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію: дис. … канд. юрид. наук : 12.00.07. К., 2009. с.38

40. Мельник С.В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016. Т. 55. №5. С. 187–197

41. Моніторинг спільного телемарафону «Єдині новини» за 17 жовтня 2022 року. Ігор Куляс. URL: https://detector.media/shchodenni-telenovini/article/204044/

42. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. Віче. 2007. №12. С. 23-25.

43. Начальник штабу полку «Азов» Богдан Кротевич «Тавр» про оборону Маріуполя, зрадників, полон, здивованих "фсбешників" та чи можна деокупувати Крим. URL: https://bukinfo.com.ua/interv-yu/nachalnyk-shtabu-polku-azov-bogdan-krotevych-tavr-pro-oboronu-mariupolya-zradnykiv-polon-zdyvovanyh-fsbeshnykiv-ta-chy-mozhna-deokupuvaty-krym.

44. Найдьонова Л.А. Кібер-булінг або агресія в інтернеті: способи розпізнання і захист дитини. Методичні рекомендації. Серія: На допомогу вчителю. 2011. Вип. 4. 34 с

45. Німецькі поборники приватності угледіли загрозу в соціальній мережі Facebook, а точніше в улюбленій користувачами кнопці like. URL: http://briz.if.ua/9590. htm (дата звернення: 08.09.2017)

46. Нове замовчування війни: Instagram приховує дописи з хештегами про воєнні злочини Росії. URL: https://speka.media/viina-rosiyi-proti-ukrayini/nove-zamovchuvannya-vijni-instagram-prihovuye-dopisi-z-heshtegami-pro-vijskovi-zlochini-rosiyi-9w74qp

47. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні. Право і суспільство. 2012. № 3. С. 132-137.

48. Основи інформаційного права України: навч. посіб. / Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін.; За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К.: Знання, 2004. С. 274.

49. Орбан-Лембрик Л. Б. Соціальна психологія: Навч. посіб. К.: Академвидав, 2005. С. 448.

50. Очі Єрмака всюди! Як друзі голови ОП отримують важливі посади. URL: https://www.youtube.com/watch?v=zubpzKefDZc&t=1500s&ab_channel=BIHUSInfo.

51. Пастернак-Таранушенко Г.А. Економічна безпека держави. Методологія забезпечення: Моногр. К.: Київ. екон. ін-т менедж., 2003. 320 с.

52. «Перша світова медійна війна». З якою назвою напад Росії на Україну увійде в історію і що робити з 9 травня – інтерв'ю з Антоном Дробовичем. URL: https://nv.ua/ukr/world/geopolitics/viynav-ukrajini-persha-svitova-mediyna-viyna-drobovichnovini-ukrajini-50235840.html.

53. Петрик В.М. Забезпечення інформаційної безпеки держави: підручник; за заг. ред. О.А. Семченка та В.М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. С. 672.

54. Петрик В. Канарський Ю. Методи гібридної війни Росії проти України. Напрями протидії. Information Technology and Security. 2015. Vol. 3, № 1. С. 30-37.

55. Петрицький А.Л. Інформаційне законодавство України: актуальні проблеми та шляхи їх вирішення. Вісник Маріупольського державного університету. Серія: право. 2013. Вип. 5. С. 64-68.

56. Плачинда С. Словник давньоукраїнської міфології. К.: Велес, 2007. С. 181–182.

57. Постанова НБУ № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській

системі України» від 28.09.2017. Верховна Рада України : офіційний вебсайт. URL: http://zakon3.rada.gov.ua/laws/show/v0095500-17.

58. Почепцов Г. Гібридна війна: інформаційна складова. URL: http://osvita. mediasapiens.ua/trends/1411978127/gibridna_viyna_informats iyna_skladova/ (дата звернення: 23.12.2017).

59. Проект Закону про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету) URL: http://w1.c1. rada.gov.ua/pls/zweb2/ webproc4_1?pf3511=50669. (дата звернення: 19.08.2017).

60. Про авторське право і суміжні права: Закон України від 23 грудня 1993 р. № 3792-12. ВВР України. 1994. № 13. Ст.64.

61. Про бібліотеки і бібліотечну справу: Закон України від 27 січня 1995 р. № 383- 18. ВВР України. 2014. № 14. Ст.252.

62. Про введення воєнного стану в Україні. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення 20.04.2022).

63. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції. Закон України. URL: https://zakon.rada.gov.ua/ laws/show/2110-20#Text (дата звернення 20.04.2022).

64. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення 20.04.2022).

65. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів

України військових формувань, вчиненому в умовах воєнного або надзвичайного стану. URL: https://zakon.rada.gov.ua/laws/show/2160-20#n10 (дата звернення 20.04.2022).

66. Про державну підтримку засобів масової інформації та соціальний захист журналістів: Закон України від 23.09.1997 р. № 540/97-вр. ВВР України. 1997. № 50. Ст. 302.

67. Про державну таємницю: Закон України від 21.01.1994 р. ВВР України. 1994. № 16. Ст.93.

68. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. ВВР України. 2003. № 36. Ст.275.

69. Про електронний цифровий підпис: Закон України від 22.05.2003 р. № 852-IV. ВВР України. 2003. № 36. Ст.276

70. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98. ВВР України. 1998. № 27-28. Ст.182

71. Про національний архівний фонд і архівні установи: Закон України від 24.12.1993 р. №3814-XII. ВВР України. 1994. № 15. Ст.86.

72. Про Національну програму інформатизації: Закон України від 4.02.1998 р. № 74/98. ВВР України. 1998. № 27-28. Ст.181.

73. Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23.09.1997 р. № 538/97. ВВР України. 1997. № 48. Ст. 296.

74. Про невідкладні заходи щодо забезпечення інформаційної безпеки України: Рішення, затв. Указом Президента від 23.04.2008 р. № 377/2008. URL: http:// zakon3.rada.gov.ua/laws/show/377/2008.

75. Про основи національної безпеки України : Закон України : від 19.06.2003 р. № 964-IV. ВВР України. 2003. № 39.

76. Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки : Закон України від 9.01.2007 р. № 537-V. ВВР України. 2007. № 12. Ст. 102.

77. Про рекламу: Закон України від 3.07.1996 р. № 270/96-ВР. ВВР України. 1996. № 39. Ст. 18.

78. Про Суспільне телебачення і радіомовлення України: Закон України від 17.04.2014 р. № 1227-VII. Відомості Верховної Ради. 2014. № 27.

79. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. ВВР України. 1994. № 10.

80. Про засади інформаційної безпеки України: проект Закону України від 28.05.2014 р. № 4949. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JG3TH00A.html.

81. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Рішення РНБО, введено в дію Указом Президента № 449/2014 від 01.05.2014. URL: http://zakon0.rada.gov.ua/laws/show/ n0004525-14.

82. Про зв'язок: Закон України (втратив чинність) від 16.05.1995 р. №160/95-вр. ВВР України. 1995. № 20. Ст.143.

83. Реінтеграція окупованих територій: інформаційна складова. URL: https://od.org.ua/uk/.

84. Система управління "Дзвін-АС" стала на озброєння України. URL: https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny/

85. Ситник Г. Безпека як інтегральна характеристика розвитку соціальних систем. Державне управління в Україні: реалії та перспективи: зб. наук. праць. К., 2005. С. 278-282.

86. Словник синонімів української мови. URL: http://synonyms_uk.enacademic.com/ (дата звернення: 22.10.2017).

87. Солодка О.М. Щодо окремих організаційно-правових питань забезпечення інформаційної безпеки України URL: http://stratcom.co.ua/shhodo-okremihorganizatsijno-pravovih-pitan-zabezpechennya-informatsijnoyi-bezpeki-ukrayini/ (дата звернення: 01.09.2017).

88. Статистика платіжного шахрайства — результати 2017-го року (ІНФОГРАФІКА). Українська міжбанківська асоціація членів платіжних систем ЕМА : вебсайт. URL: https://ema.com.ua/cyberfraud-ema-statistics-results2017/

89. Стратегія кібернетичної безпеки України, затв.Указом Президента України від 15 березня 2016 року № 96/2016. URL: http://zakon3.rada.gov.ua/laws/show/96/2016.

90. Тихий В. П. Поняття безпеки людини і її правове забезпечення. Вісник Асоціації кримінального права України. 2016. № 1(6). С. 21-40.

91. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : Моногр. / заг. ред. Р.А. Калюжний. К.: Центр навч.-наук. та наук.- практ. вид. НА СБ України, 2014. С. 196.

92. Требін М. П. «Гібридна» війна як нова українська реальність. Український соціум. 2014. № 3. С. 113-127.

93. У Донецьку заблокували 39 сайтів українських інтернет-видань URL: http:// zik.ua/ua/news/2015/06/09/u_donetsku_zablokuvaly_39_saytiv_ukrainskyh_ internetvydan_597122 (дата звернення: 19.10.2017).

94. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/ show/685/2021#n7.

95. Український супутник компанії ICEYE вже дає результати на полі бою – Міноборони. URL: https://mil.in.ua/uk/news/ukrayinskyj-suputnyk-kompaniyi-iceye-vzhe-daye-rezultaty-na-poli-boyu-minoborony/].

96. Уряд дозволив закладам культури відновити роботу в умовах війни. URL: https://zaxid.net/ uryad_dozvoliv_zakladam_kulturi_vidnoviti_robotu_v_ umovah_viyni_n1539889.

97. Філософія. Навч. посіб. / За заг. ред. Ю.В. Осічнюка. К.: Атіка, 2003. С. 464.

98. Фурашев В.М. Законодавче забезпечення інформаційної безпеки України Інформація і право. 2014. №1(10). С. 59-66.

99. Хворост Х.Ю. Інформаційно-психологічний вплив у розрізі безпеки здоров'я. Наука і освіта. 2016. №2-3. с.184-191.

100. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. Демокр. врядування. 2014. Вип. 13. URL: http://lvivacademy.com/ visnik13/zmist.html (дата звернення: 03.05.2017).

101. Щодо інформаційно-психологічної складової агресії Російської Федерації проти України (за результатами подій 1-2 березня 2014 року). Аналітична записка Національний інститут стратегічних досліджень URL: http://www.niss.gov.ua/ articles/1476/ (дата звернення: 28.03.2015)

102. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану. Рішення РНБО. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text (дата звернення 20.04.2022).

103. Ященко В. А. Щуровський А. М. Національна та державна безпека : діалектика взаємозв'язку. Державна безпека України. 2004. № 1. С. 19-20.

104. «Воєнний стан в Україні продовжать на 90 днів». URL: [https://suspilne.media/312618-voennij-stan-v-ukraini-prodovzat-na-90-dniv/].

105. «Мова ворожнечі»: як не абсолютизувати ані її уникання, ані правомірного використання під час війни? URL: http://detector.media/infospace/article/122037/2017- 01-08-mova-vorozhnechi-yak-ne-absolyutizuvati-ani-ii-unikannya-anipravomirnogo-vikoristannya-pid-chas-viini/ (дата звернення: 03.09.2017).

106. «Інформаційний вплив: теорія і практика прогнозування» : Моногр. / За ред. П.Д. Фролова. К.: Міленіум, 2011. С. 47.

107. «Інформаційні виклики гібридної війни: контент, канали, механізми протидії» : аналіт. доп. / за заг. ред. А. Баровської. К.: НІСД, 2016. С. 109.

108. «ОПЗЖ не працює. Що буде з Інтером?». Сайт редакції Детектор медіа. URL: https://detector.media/infospace/article/198490/2022-04-18-opzzh-ne-pratsyuie-shchobude-z-interom/ (дата звернення 20.04.2022).

109. «Проблеми забезпечення та розвитку прав людини в умовах інформаційного суспільства. Український часопис міжнародного права». Сухорольський П. 2013. № 1. С. 21.

110. «Сміх продовжує життя, але ракети сильніші». Квартал 95, Леви на Джипі, Дантес та стендап-коміки про війну та жарти. URL: https://suspilne.media/257788-smih-prodovzue-zitta-ale-raketi-silnisi-kvartal-95-levi-na-dzipi-dantes-ta-stendap-komiki-pro-vijnu-ta-zarti/.

111. «Стратегія інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення 20.04.2022).

112. Butlin J. Our common future. Journal of International Development. London, Oxford University Press, 1987. pp. 284–287.

113. Google виділить $10 мільйонів на боротьбу з фейками про війну Росії проти України. URL: https://ms.detector.media/it-kompanii/post/29444/2022-05-06-google-vydilyt-10-milyoniv-na-borotbu-z-feykamy-pro-viynu-rosii-proty-ukrainy/.

114. Hartmann F. H. The relations of nations. London: Macmillan, 1962. 710 p.

115. How Many Ads Do We See A Day In 2022? URL: https://lunio.ai/blog/strategy/how-many-ads-do-we-see-a-day/.

116. Hybrid Warfare URL: http://www.gao.gov/assets/100/97053.pdf (Last accesed: 15.10.2017).

117. Liderman K. Bezpieczeństwo informacyjne. Warszawa, Wydawnictwo Naukowe PWN, 2012. 216 s.

118. Liedel K. Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego. Torun: Wyd-wo Adam Marszałek, 2014. 96 s.

119. Redefining Information Warfare Boundaries for an Army in a Wireless World URL: http://www.rand.org/content/dam/rand/pubs/monographs//MG1100/MG1113/ RAND_ MG1113.pdf (Last accesed: 15.10.2017.

120. Russia Today і Sputnik заборонено у всіх країнах ЄС URL: https://www.nrada.gov.ua/u-vsih-krayinah-yevrosoyuzu-zaboronyv-russia-today-sputnik1/.

121. This is hilarious. "Bucha" in Yandex VS Google URL: https://twitter.com/timsoulo/status/1510955352267063296.

122. Toffler A. War and Anti-War. N.Y. : Little, Brown and Company, 1993. 302 p.

123. Trend Report «Financial Cyber Threats Q1 2017» ElevenPaths : web-site. URL: https://www.elevenpaths.com/wp-content/uploads/2017/04/ Financial_Threats_Q1-2017_EN.pdf.

124. Ukraine Now and Forever: Держава презентує об’єднаний бренд української культури в світі #StandWithUkraine. URL: https://ck-oda.gov.ua/ novyny-cherkaskoyi-oblasti/ukraine-now-and-foreverderzhava-prezentuye-obyednanij-brend-ukrayinskoyikulturi-v-sviti-standwithukraine/.].

125. Wallerstein I. Analiza systemów-światów. Wprowadzenie. Warszawa, 2007. 160 s.

126. World Internet Users and Population Stats. URL: www.internetworldstats. com.stats. htm (Last accesed: 15.10.2017)],

127. Zięba R. Instytucjonalizacja Bezpieczeństwa europejskogo. Warszawa; Scholar, 2001. 406 s. c.27.

ДОДАТКИ

Додаток А

№ п/п	Назва псевдоукраїнського Телеграм-каналу, який працює в інтересах рф
1	Крокодил
2	ШептунUAУкраина Война
3	Легитимный
4	Анатолий Шарий
5	Резидент
7	#МОНТЯН!
8	ЗеРада
9	Open Ukraine | Открытая Украина
10	UKR LEAKS
12	Сплетница
14	Картель
15	ОЛЬГА ШАРИЙ
17	Украина.ру
18	MediaKiller
20	ТелеДНО
21	Женщина с косой
22	Типичная Одесса
23	Война с фейками
24	Главное в Херсоне
27	Чёрный Квартал
28	НачШтабу
29	Бунтарь
30	наглый
31	Украина. Спецоперация. Мониторинг
32	Я ♡ Краматорск
33	Одесский фраер
34	Запрещённая Украина
35	Отряд Ковпака
36	Шкварка News
38	Кріт СБУ
39	щибуля UA
40	Администрация города Мелитополя
41	Лисичанск. Северодонецк. Рубежное.
42	Dirty Harry | Игорь Гомольский
43	Партия Шария
44	Черговий ООС
45	Нетипичное запорожье
46	Новости Херсонщины
47	Главное в Геническе
48	Херсон Life Новости
49	Украинский формат
50	Главное в Мелитополе
51	Тень на плетень
52	Нетипичное Запорожье
53	Херсон live
55	Николаев live
56	Тремпель Харьков
57	ХтоШо
58	93 бригада "Холодний Яр" | ОБРАТНАЯ СТОРОНА
59	Главное в Чернобаевке
60	Новый Мелитополь
61	Military photographer
62	ЗЕландия
63	ХЕРСОН сегодня
64	Херсонский Вестник
66	Главное в Каховке и Новой Каховке
67	Главное в Скадовске
68	Чернигов
69	Сумы
70	Глухов
71	Бровары
72	Шостка
73	Васильков
74	Новгород-Северский
75	Нежин
76	Обухов
77	Белая Церковь
78	Овруч
79	Ромны
80	Носовка
81	Славутич
82	Бахмач
83	Прилуки
84	Ирпень
85	Березань
86	Ахтырка
87	Конотоп
88	Бердянск ZaVtra
89	Новый Мелитополь
90	Южный плацдарм
91	Энергодарский связной
92	Энергодар Тудей
93	Токмак Сегодня
94	Главное в Пологах
95	Главное в Энергодаре
96	Главное в Бердянске
97	Харьковские антифашисты
98	Друзья Алексея Селиванова
99	Администрация города Васильевка
100	Нетленка

(назви псевдо українських телеграм-каналів, які працюють в інтересах РФ)

Додаток Б

URL: https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny/