МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ХАЄЦЬКА ЯНА ВІКТОРОВНА

Допускається до захисту:
завідувач кафедри
політології
та державного управління
д.політ.н., доцент
_____Чальцева О.М.
«____»_____20__р.

ДЕРЖАВНА ПОЛІТИКА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Спеціальність 052 Політологія

Бакалаврська робота

Науковий керівник:
Чальцева О.М., завідувач кафедри
політології
та державного управління
д.політ.н., доцент

Оцінка:_____/____/ _____
(бали/за шкалою ЄКТS/за національною шкалою)

Голова ЕК:

_____
(підпис)

Вінниця 2021

АНОТАЦІЯ

Хаєцька Я. В. Державна політика національної безпеки в інформаційній сфері

Дипломна робота присвячена дослідженню питання інформаційної безпеки держави через з'ясування сутності інформаційного захисту людини, суспільства, держави як важливої складової частини національної безпеки України в умовах гібридної війни. Зазначено, що сьогодні в Україні фактично відсутня система інформаційної безпеки, яка б могла забезпечити виявлення, аналіз інформаційних загроз національній безпеці, а також протидію цим загрозам. Стверджується, що інформаційна складова частина є безумовним об'єктом маніпулювання в умовах гібридної війни, адже складна політична ситуація, в якій перебуває Україна останні шість років, постійне погіршення іміджу держави на міжнародній арені зумовлені низкою чинників, серед яких важливим фактором є неналежний стан системи інформаційної безпеки. Забезпечення інформаційної безпеки сьогодні стає важливою складовою частиною національної безпеки України. Основними складовими елементами інформаційної безпеки автор називає забезпечення якісного інформування громадян, вільного доступу до різних джерел інформації, захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства.

У роботі зазначено, що забезпечення інформаційної безпеки завдяки послідовній реалізації чітко сформульованої національної інформаційної стратегії значною мірою може сприяти забезпеченню досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Так, втілення у життя вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних і військових конфліктів. Автор доводить, система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни і становить сукупність органів державної влади,

недержавних структур і громадян, котрі повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам за сучасних умов.

Ключові слова: інформація, інформаційна безпека, державна інформаційна політика, загрози інформаційній безпеці, національна безпека, стратегія національної безпеки.

Khayetskaya Y. V. State National Security Policy in the Informational Field

The is devoted to the study of information security of the state. The essence of information protection of human, society, state as an important component of national security of Ukraine in the conditions of hybrid war is revealed. It is noted that in Ukraine there is practically no information security system that could provide detection, analysis of information threats to national security, as well as counteracting these threats.

It is claimed that information is the object of manipulation in the context of the hybrid war that is taking place in Ukraine today. This is explained by the fact that the difficult political situation in which our country has been for the last six years, the constant deterioration of the state image in the international arena, are caused by a number of factors, among which is the poor state of the national information security system. Information security is becoming an important component of Ukraine's national security today. The author calls the main components of information security the provision of quality information to citizens, free access to various sources of information, and protection against negative information influences. The totality of these elements should promote the unity of society. The work states that providing information security through the consistent implementation of a clearly formulated national information strategy can help ensure success in solving problems in political, military, political, military, social, economic and other spheres of state activity.

Implementing the right information policy can influence the resolution of internal political, external political and military conflicts. The author argues that the system of information security of the state is an integral part of the general system of national security of the country and is a collection of state authorities, non-governmental organizations and citizens. Together they should carry out activities to ensure information security on the basis of legal norms, effectively withstand information threats in the current conditions.

Key words: information, information security, state information policy, threats to information security, national security, strategy of national safety.

ЗМІСТ

ВСТУП

Актуальність нашого дослідження. В Україні, як і в усьому світі, проблеми забезпечення системи безпеки держави, суспільства й особистості все більше виходять на перший план у державній політиці та державному управлінні. Інформаційна безпека належить до числа пріоритетних цілей сучасної держави і є одним з основних факторів його стабільного розвитку.

Очевидно, що системні дефекти та збоїв у функціонуванні механізмів забезпечення інформаційної безпеки можуть привести до соціально-політичних, економічних і техногенних зрушень, здатних підірвати можливість органів державного управління належним чином здійснювати свої основні функції. Інформаційна безпека суспільства в цілому та його структурних частин – досить актуальна проблема.

Це пов'язано з тим, що питання інформації та особливо соціальної інформації в даний час стали особливо важливими. Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, яка є важливим чинником суспільного життя, багато в чому визначає перспективи успішної реалізації соціально-політичних і державно-управлінських перетворень українського суспільства.

Це обумовлено наступними основними обставинами: інтенсивним розвитком інформаційної інфраструктури і, насамперед, інформаційно-телекомунікаційних систем, засобів і систем зв'язку, інтеграцією у світовий інформаційний простір, а також інформатизацією практично всіх аспектів суспільного життя, діяльності органів державної влади і управління, що значно підвищило залежність ефективного функціонування суспільства та держави від стану інформаційної сфери; індустрією інформатизації, телекомунікацій і зв'язку, демократизації тощо.

Сучасні соціальні перетворення передбачають активну участь держави у розвитку інформаційного суспільства та актуалізують проблему наукового аналізу державного управління інформаційною сферою.

Інформаційна сфера як надзвичайно складна система відносин з приводу звернення інформації в суспільстві і державі є об'єктом наукових досліджень російських вчених: Швеця М.Я., Калюжного Р.А., Брижка В.М., Гавловського В.Д., Кормича Б.А., Кушакової Н.В, Макаренко Д.В., Орлова К.І., Почепцова Г.Г., Хахановського В.Г., Цимбалюка В.С., Фурашева В.М. та інших. У їх працях аналізуються правові, організаційні та технічні проблеми розвитку інформаційної сфери. В той же час, окремого дослідження потребують структурно-функціональні аспекти державного управління інформаційною сферою в Україні.

Вивченню даного питання приділяли увагу багато науковців та дослідників. Зокрема, теоретичні аспекти забезпечення інформаційної безпеки розглядали такі науковці, як: В. Абакумов, В. Антонюк, В. Богуш, О. Юдін, І. Боднар, В. Брижко, М. Волошина, С. Гуцу, О. Дзьобань, К. Захарченко, Р. Калюжний, О. Литвиненко, В. Ліпкан, Л. Наливайко, В. Петрик, О. Рижук та ін.

Зарубіжний досвід був проаналізований такими науковцями, як: О. Горелихина, Т. Михайлюк, О. Рябоконь, І. Чернухін, С. Шустенко, Є. Макаренко та ін. Ряд науковців зробили спробу виділити проблеми забезпечення інформаційної безпеки та запропонувати шляхи їх вирішення, зокрема: О. Горбатюк, У. Ільницька, В. Антонюк, Т. Ткачук, І. Беззуб, В. Горбулін, М. Еделєва та ін. Дисертаційні роботи виконали такі науковці, як: В.Гурковський, О. Довгань, В. Козубський, Є. Макаренко, О. Олійник, О. Петкова та ін.

Незважаючи на це розвиток механізмів забезпечення інформаційної безпеки потребує подальшої розробки та наукового обґрунтування шляхів їх модернізації, що зумовило вибір теми, мету та завдання наукового дослідження.

Мета роботи є дослідження державної політики та національної безпеки в інформаційній сфері.

Об'єк нашого дослідженя національна безпека в інформаційній сфері.

Предметом дослідження є національна безпека в інформаційній сфері України.

Відповідно до мети дипломного дослідження нами було **поставлено такі завдання:**

1. Дослідження стану державного управління інформаційною сферою в Україні.
2. Визначити основні концепції державної інформаційної політики.
3. Провести аналіз державної політики у сфері інформаційної безпеки.
4. Державна інформаційна політика України та шляхи її вдосконалення.
5. Аналіз можливостей впровадження кращих міжнародних та національних практик в Україні формування та реалізації державної політики інформаційної безпеки.
6. Запропонувати перспективні напрямки застосування механізмів реалізації державної політики інформаційної безпеки в Україні.
7. Окреслити коло відповідальних органів та шляхи вдосконалення системи інформаційної безпеки України.

Методи дослідження. Для виконання завдань дослідження використовувалися загальнонаукові та спеціальні методи:

1. Аналіз і синтез – для деталізації об'єкта дослідження.
2. Узагальнення-для виявлення теоретико-методологічних засад механізмів інформаційної безпеки.
3. Порівняльний метод для вивчення нормативно – правового забезпечення інформаційної безпеки.

4. Метод моделювання – для розробки перспективних напрямів застосування механізмів реалізації державної політики інформаційної безпеки та можливих шляхів удосконалення системи інформаційної безпеки України.

5. Абстрактно-логічний метод – для теоретичного узагальнення та формулювання висновків і пропозицій.

Структура роботи. Дипломна робота складається із вступу, основної частини, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1. КАТЕГОРІЇ ТА СУТНІСТЬ ІНФОРМАЦІЙНОЇ СФЕРИ В УКРАЇНІ

1.1 Інформаційна безпека: визначеня і сутність

В умовах глобальних викликів головним стратегічним національним ресурсом, що визначає економічну і оборонну міць держави, є інформація та інформаційні технології, від яких вирішальною мірою залежать всі сфери життєдіяльності суспільства: виробництво та управління, оборона і енергетика, транспорт і зв'язок, банківська справа і фінанси, наука, освіта і багато інших.

Необхідність забезпечення інформаційної безпеки визначається необхідністю забезпечення національної безпеки України в цілому, наявністю таких загроз інформаційній сфері країни, які можуть завдати істотної шкоди загальним національним інтересам, з урахуванням того, що інформація може вплинути на зміни у свідомості та поведінці людей. Завданням інформаційної безпеки є створення системи протидії інформаційним загрозам та захисту власного інформаційного простору держави, інформаційної інфраструктури та інформаційних ресурсів. При виникненні криз і ескалації конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї [14].

Актуальність проблеми забезпечення інформаційної безпеки зумовлена також необхідністю прийняття ефективних управлінських рішень, адекватних політичним завданням таблиця 1.1.

Таблиця 1.1

Дослідження актуальності проблеми забезпечення інформаційної безпеки

№	Розкриття проблеми забезпечення інформації
1	По-перше, відзначимо, що залежність від інформації та інформаційних технологій стає одним з якісних станів формування суспільства. Володіння своєчасними, точними і достовірними даними є надзвичайно важливим фактором ефективності прийняття управлінських рішень. Інформація стає стратегічним ресурсом в системі державного управління. Стан правового регулювання суспільних відносин у цій сфері багато в чому визначає рівень розвитку держави.
2	По-друге, інформаційна безпека, як стан захисту інтересів особистості, суспільства і держави в інформаційній сфері, також визначає стан соціально-політичної, економічної, оборонної та інших елементів державної безпеки. Стрімкий розвиток сфери інформаційних відносин ставить в пряму залежність від них всі аспекти суспільного життя, викликаючи в ній глибокі якісні зміни. Нові інформаційні технології змінюють спосіб життя людей, змінюють характер і зміст самих категорій, які вимірюють соціальну (життєву) активність і спілкування людини. Сьогодні Інформаційні технології, інтенсивно впроваджуються в сферу політичної діяльності, бізнесу та державного управління, трансформують характер міжособистісних відносин у суспільстві, змінюють самі принципи ведення бізнесу, управління у сфері політики та економіки.
3	По-третє, забезпечення інформаційної безпеки пов'язане з питаннями забезпечення технологічної безпеки країни. Також значний інтерес представляє розгляд проблеми співвідношення можливостей засобів забезпечення безпеки та засобів несанкціонованого збору, обробки та доступу до інформаційних ресурсів, наявності протоколів взаємодії користувачів та інформації з урахуванням ступеня її важливості та секретності, стану соціально-економічної та суспільно-політичної ситуації в країні та її суб'єктах.

Питання інформаційної безпеки знаходиться в центрі уваги вчених. Водночас інформаційна безпека дещо ігнорується. На перший погляд «інформаційна безпека» і «інформаційна безпека» ідентичні за змістом, але насправді це далеко не так. У першому випадку об'єктом є інформація, у другому – безпека як частина всієї національної безпеки.

На думку Л.О. Кочубей, інформаційна безпека – це такий стан захищеності життєво важливих інтересів, а отже, й інформаційної озброєності держави, суспільства, особистості, за якого жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стій- кого прогресивного розвитку названих суб'єктів – [8, с. 221-222].

За визначенням В.В. Шемчука, інформаційна безпека – це правовідносини, що виникають під час здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства та держави [10, с. 23].

Інформаційна безпека - це стан захисту людини, суспільства або держави від інформації, яка носить шкідливий або незаконний характер, а також від інформації, яка робить негативний вплив на свідомість особистості, перешкоджає сталому розвитку особистості, суспільства і держави. Інформаційна безпека забезпечує сталий розвиток особистості, суспільства і держави і захищає інформаційну інфраструктуру (комп'ютери, інформаційно - телекомунікаційну інфраструктуру).

Проблема забезпечення інформаційної безпеки не нова. Протягом багатьох років компанія вирішує проблему створення інструментів і систем для зберігання, обробки, передачі та захисту інформації. На основі загальної концепції побудови систем інформаційної безпеки. Дана концепція повинна забезпечити єдність принципів формування та реалізації заходів державного управління на всіх етапах системи захисту інформаційної сфери.

Забезпечення інформаційної безпеки здійснюється на основі поєднання законодавчих, правоохоронних, судових, контрольних та інших форм діяльності державних органів у взаємодії з органами місцевого самоврядування, організаціями та громадянами.

Основний вектор державного управління в галузі інформаційної безпеки спрямований на виявлення і нейтралізацію існуючих ризиків інформаційної безпеки з урахуванням всіх факторів, що впливають як на державні структури, так і на інформаційні системи.

Управління інформаційною безпекою включає в себе кілька рівнів:

1.рівень міжнародних професійних асоціацій, пов'язаних з областю інформаційних технологій, телевізійного зв'язку та інформаційної безпеки.

2.рівень великих компаній, що працюють у сфері інформаційних технологій, які багато в чому визначають стан інформаційної безпеки в суспільстві

користувачів інформаційних систем, а також впливають на безпеку різних елементів інформаційної інфраструктури.

3.державний рівень-рівень державних органів, що впливають на життя суспільства, стан правової системи, розвиток економіки і технологій.

4.рівень окремих компаній - це спільнота користувачів інформаційних систем, які зацікавлені у власній інформаційній безпеці та самостійно забезпечують захист існуючих інформаційних ресурсів.

Кожен рівень зазначеної ієрархії характеризується своїми завданнями і специфічними методами організаційної роботи. Діяльність держави в галузі інформаційної безпеки, як правило, ґрунтується на загальних завданнях органів державної влади, зокрема:

1. збереження принципу державного суверенітету.

2. політична стабільність.

3. розвиток демократичних інститутів суспільства, а також забезпечення прав і свобод громадян.

4. Зміцнення правопорядку.

5. соціально-економічний розвиток країни і стійкість фінансової системи.

Питання інформаційної безпеки можна розділити на три великі групи:

- гуманітарні проблеми-проблеми інформаційної безпеки, що виникають у зв'язку з безконтрольним використанням і поширенням персональних даних громадян і вторгненнями в приватне життя;

- проблеми економічного і правового характеру – виникають в результаті втрати або крадіжки комерційної та фінансової інформації; проблеми політичного характеру – проблеми інформаційної безпеки, що виникають в результаті інформаційної війни, кібервійни та електронної розвідки в інтересах політичних груп, компрометації державних секретів, атак на інформаційні системи важливих оборонних, транспортних і промислових об'єктів.

Механізм забезпечення інформаційної безпеки держави реалізується за допомогою використання таких адміністративно-правових засобів органами виконавчої влади:

1.дозволу, в тому числі дозвіл на здійснення діяльності, пов'язаної з державною таємницею, стандартизацією заходів інформаційної безпеки, ліцензуванням і легалізацією.

2. засоби реєстрації, до яких відносяться реєстрація засобів масової інформації та державна реєстрація баз персональних даних.

3. засоби адміністративно-правового примусу, до яких слід, перш за все, віднести засоби адміністративної відповідальності.

У контексті інформаційного розвитку суспільства та забезпечення інформаційної безпеки можна виділити наступні чинники (табл. 1.2).

Таблиця 1.2

Чинники інформаційної безпеки держави

№ з/п	**Чинник**	**Характеристика**
1	Соціально- економічний чинник	Формує економічне підгрунтя інформаційного розвитку держави й суспільства та матеріально- технічні можливості впровадження інформаційно- комунікаційних технологій. Узагальнені соціально-економічні чинники (стабільний розвиток економіки, високий рівень забезпеченості населення та апарату держави необхідними для розвитку матеріально-технічними та інформаційно-комунікаційними засобами, достатній рівень фінансування сфери освіти та науки) визначають результативність процесу забезпечення інформаційної безпеки
2	Правовий чинник	Створення досконалого інформаційного законодавства, що регламентує інформаційну сферу суспільних відносин та його ефективну реалізацію (вдосконалення нормативної бази з протидії комп'ютерній злочинності, захист інформації з персональних даних і державної таємниці, підвищення рівня правової свідомості громадян в інформаційно-комунікаційній сфері)
3	Технологічний чинник	Сукупність організаційно-технічних та спеціальних засобів, що формують технічну досконаліть і сучасність засобів обробки інформації та спрямовані на ефективне функціонування інформаційної сфери (розвинена мережа швидкісного Інтернету, досконаліть інформаційних ресурсів; новітні автоматизовані системи обробки та передачі інформації)

Порівняння понять інформаційної безпеки та інформаційної безпеки дозволяє зробити висновок, що друге поняття набагато глибше по суті і ширше за змістом. Інформаційну безпеку України можна розглядати з точки зору захисту не тільки інтересів держави, але в першу чергу особистості і суспільства [20].

О.І. Крюков пропонує під інформаційною безпекою розуміти публічно-правові відносини, які стосуються процесу створення організації, підтримки, захисту та охорони безпечних умов, необхідних людині (фізичній або юридичній особі, установі, підприємству, організації), суспільству і стану їх життєдіяльності; публічно-правові відносини, пов'язані з організацією технологій створення, поширення, зберігання та використання інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, Суспільства, держави [7].

Н. Р. Нижник розуміє інформаційну безпеку як стан правових норм і відповідних інститутів безпеки, що гарантують постійну доступність даних для прийняття стратегічних рішень і захисту інформаційних ресурсів країни [9]. Фурашев в. вважає, що інформаційна безпека-це вид суспільних інформаційних правовідносин щодо створення, підтримки, захисту та охорони безпечних умов життя, бажаних для людини, суспільства і держави [5]. Також до цієї групи досліджень слід включити трактування сутності інформаційної безпеки в нормативних правових актах України.

Так, у третьому розділі закону України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" визначено, що "інформаційна безпека-це стан захисту життєво важливих інтересів людини, суспільства і держави, при якому запобігається шкоди через: неповноту, невчасність і неправдоподібність використовуваної інформації; негативного інформаційного впливу; негативні наслідки застосування інформаційних

технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності Інформації" [27].

В ході розробки проекту Закону України" Про засади інформаційної безпеки України " було запропоновано наступне визначення: Інформаційна безпека-це стан захисту життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається шкода внаслідок неповноти, несвоєчасного і ненадійного поширення інформації, порушення цілісності та доступності інформації, несанкціонованого поширення інформації з обмеженим доступом., а також шляхом негативного інформаційно-психологічного впливу та умисного заподіяння негативних наслідків використання інформаційних технологій [19].

У рамках третього напрямку досліджень – "соціально – політичне" - проводиться аналіз політичних аспектів забезпечення інформаційної безпеки та вивчення проблем захисту суб'єктів інформаційної безпеки від негативного інформаційного впливу. Джебан О.П. та Пилипчук В. Г., які визначають інформаційну безпеку як стан захисту життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, що забезпечує їх сталий розвиток [40].

Цікаві визначення інформаційної безпеки такими авторами, як О.Данилян, о. Дзебан, м. Панов, які у своєму підручнику "національна безпека України: сутність, структура та напрями реалізації", де інформаційна безпека визначається як захист об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією, та нерозголошення даних про конкретний об'єкт, що становить державну таємницю.

Важливо, що автори акцентують увагу на проблемі інформаційних воєн, оскільки сьогодні це ефективний і цивілізований спосіб колонізації однієї країни іншої і виділяють додатково такі загрози інформаційній безпеці, як розголошення інформації, що становить державну таємницю, вплив засобів масової інформації

на свідомість людини і суспільства, забезпечення державних організацій повною, достовірною і своєчасною інформацією, необхідною для прийняття рішень, а не інтеграція України у світове інформаційне поле., недостатня кваліфікація та активність українських інформаційних служб, використання інформаційних технологій злочинцями тощо [38].

Як національна безпека та безпека держави "Інформаційна безпека розглядається як стан інформаційної безпеки держави (захист об'єкта від інформаційних загроз), при якому негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій або спеціальних інформаційних операцій, актів зовнішньої інформаційної агресії і таємного видалення інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп'ютерні злочини не завдають істотної шкоди національним інтересам держави і не перешкоджають стабільному розвитку інформаційної інфраструктури, правильному функціонуванню національного інформаційного простору України і всіх пріоритетних сфер життєдіяльності" [8].

Богуш в.визначає, що інформаційна безпека-це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій і держави [12]. Дуже близьким семантично є визначення Фісун А. П. І. Більовської Ю. А. – "стан безпеки інформаційної середовища, що відповідає інтересам держави, що забезпечує формування, використання і розвиток можливостей незалежно від впливу внутрішніх і зовнішніх інформаційних загроз" [7].

У сучасних умовах інформація є, без перебільшення, одним з найважливіших ресурсів розвитку цивілізації, оскільки вона активно впливає на всі сфери життя окремих суспільств і держав, а також всього світового співтовариства за допомогою розвитку інформаційно-комунікаційних технологій

(далі-ІКТ). При цьому інформація може бути використана не тільки на благо, а й на шкоду інтересам особистості, суспільства і держави [3].

Це пов'язано з тим, що ІКТ є важливим фактором глобальної інтеграції, соціального розвитку та економічного зростання, будучи найсильнішим каталізатором обміну інформацією, такі технології несуть в собі безліч явних і прихованих загроз.

У зв'язку з цим питання визначення дихотомічності та забезпечення інформаційної безпеки, визнані в нашій країні однією з найважливіших складових національної безпеки, набувають надзвичайного значення, оскільки інформаційна безпека в сучасному постіндустріальному світі впливає на тактичні та стратегічні рішення держави.

На державному рівні та в експертному науковому співтоваристві [8] існує думка, що статус члена інформаційного суспільства не змінює того факту, що кожна з країн має свої національні інтереси в інформаційній сфері і, отже, існує необхідність забезпечення безпеки цих інтересів. Однак якщо вчені приділяють значну увагу технічним аспектам забезпечення такої безпеки, то соціально-політичні та управлінські аспекти цієї проблеми, на жаль, недостатньо систематично вивчені.

На наш погляд, цей факт відображає уповільнення динаміки реформування українського суспільства, а в багатьох сферах-стагнацію цих процесів. В юридичній науці термін "інформаційна безпека" в основному використовується у вузькому – технологічному – сенсі, який притаманний, наприклад, англосаксонській правовій системі [1]. Фактично під безпекою розуміється стан захищеності інформаційно - допоміжної інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати шкоди суб'єктам інформаційних відносин (власникам і користувачам інформаційно-допоміжної інфраструктури) [12].

Метою забезпечення інформаційної безпеки держави є досягнення стану захищеності суспільних відносин від прояву зовнішніх і внутрішніх загроз, пов'язаних з інформацією та інформаційною інфраструктурою, в процесі захисту національних цінностей, реалізації національних інтересів і досягнення національних цілей. Доцільним убачається виділити такі основні групи інформаційних відносин (див. табл. 1.3.).

Таблиця 1.3.

Групи інформаційних відносин

Група відносин	Форма представлення інформації	Функція інформації
Товарно-грошові відносини	Повідомлення	Товар, послуга або об’єкт прав інтелектуальної власності
Духовні відносини	Відомості	Засіб впливу на психічний стан суб’єктів
Відносини у сфері соціального та державного управління	Відомості та повідомлення	Засіб ідентифікації суб’єктів, регулювання їх діяльності
Відносини в галузі управління технічними й технологічними системами	Повідомлення	Засіб забезпечення узгодженого функціонування окремих складових систем
Відносини, пов’язані з повсякденним міжособистісним спілкуванням	Відомості	Засіб самовдосконалення суб’єктів, їхнього інформаційного збагачення

Перелічені інформаційні відносини породжуються інтересами суб’єктів, реалізованими в інформаційній сфері.

На нашу думку, варто виокремити такі три основні групи вказаних інтересів:

- вільно володіти інформацією;
- передавати окремі масиви інформації певним суб’єктам;
- приховувати окремі масиви інформації від інших суб’єктів.

Реалізуючи ті чи інші інтереси в інформаційній сфері, суб’єкт взаємодіє з іншими суб’єктами, певним чином оформлюючи ці відносини, тобто, дотримуючись визначеного порядку їх здійснення.

Цей правопорядок залежить від рівня розвитку інформаційної інфраструктури, а також засобів, якими може оперувати суб’єкт для реалізації

його інтересів. У цивільно-правових відносинах відповідна взаємодія зазвичай набуває форми угоди, об'єктом якої є послуга, а в публічних відносинах – вимоги або звернення.

Розглянемо детальніше можливі форми такої взаємодії. Взаємодія, пов'язана з пошуком інформації. Така взаємодія може відбуватися або у формі угоди, змістом якої є надання посередницької послуги в пошуку повідомлень, що мають необхідні ознаки (оформлення, зміст матеріальної чи духовної сфери життя суспільства, рівень теоретичного узагальнення відомостей, мова, якою представлені дані, тощо), або шляхом надання можливості суб'єкту взаємодії самостійно добирати необхідні йому повідомлення.

Соціальним результатом такої взаємодії може бути як визначення місця зберігання повідомлень, котрі відповідають пошуковим ознакам конкретного суб'єкта, який володіє цими повідомленнями, отримання дозволу на доступ до цих повідомлень, так і відмова суб'єктові в наданні такого доступу або неможливість встановити місце зберігання шуканих повідомлень. Взаємодія, що має на меті отримання повідомлень, здійснюється у формі угоди, зміст якої - надавання послуг з передавання необхідних повідомлень, а взаємодія, що має на меті зберігання повідомлень – це послуги щодо забезпечення збереження наявних повідомлень. Соціальним результатом цих взаємодій буде отримання необхідних повідомлень, збереження фізичних властивостей матеріального носія, на якому вони закріплені, й, відповідно, можливість ознайомлюватися зі змістом 106 повідомлень.

Взаємодія, що має на меті використання повідомлень для отримання відомостей, здійснюється у формі угоди, зміст якої – надавання можливості ознайомлюватися з важливими для суб'єкта повідомленнями.

Соціальний результат цієї взаємодії полягає в перетворенні повідомлення у відомості, які відображаються в «інформаційній моделі» суб'єкта. Взаємодія, що

має на меті передавання (поширення) відомостей, здійснюється у формі угоди, зміст якої - надавання послуги із закріплення повідомлення, що містить трансльовані відомості, на матеріальному носії, а також передавання (доведення) повідомлення до певних суб'єктів або невизначено великої кількості суб'єктів у певний спосіб (розсилка поштою, агітація і пропаганда, розміщення на рекламних щитах, поширення повідомлень у радіо- і телепрограмах, в інших ЗМІ, розміщення на веб-сайтах тощо).

Соціальний результат цієї взаємодії – доставляння повідомлення адресатам або ознайомлення адресатів із повідомленням, що за певних обставин може зумовити зміну їхньої поведінки. Взаємодія, що має на меті оброблення інформації. Іноді фахівці виокремлюють ще один вид інформаційних відносин, - що виникають у процесі взаємодії, котра має на меті оброблення інформації.

Під обробленням інформації зазвичай розуміють перетворення певної сукупності повідомлень у нове повідомлення (безліч повідомлень), яке здійснює суб'єкт безпосередньо чи за допомогою технічних засобів, послуговуючись заздалегідь заданими алгоритмами або без них. Така взаємодія може здійснюватися у формі угоди, що полягає в наданні інформаційної (наукової, творчої) послуги, а її соціальний результат – нове повідомлення чи відомість.

Взаємодію, що має на меті оброблення інформації, можна розглядати як різновид взаємодії, що має меті володіння відомостями, за якої частина операцій із підготовки повідомлень до сприйняття суб'єктами здійснюється за допомогою обчислювальної техніки.

У публічних правовідносинах взаємодія відбувається для задоволення інтересів особи й суспільства, пов'язаних з інформацією, якою володіє держава, а також інтересів держави, що стосуються інформації, котрою володіють особи та організації, органи місцевого самоврядування, які становлять основу громадянського суспільства

Впровадження в практичне русло визначених пріоритетів державної політики в інформаційній сфері потребує великих зусиль уряду та матеріальних вкладень, яких сьогодні в державі обмаль, що, своєю чергою, потребує формування збалансованої державної політики й ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері, розроблення механізму її реалізації.

Узагальнюючи підходи до розкриття змісту категорії «інформаційна безпека держави», можна визначити основні її особливості:

1. Є складовою національної безпеки та швидко розвивається як в Україні, так і в світі, глобальна інформатизація охоплює всі сфери держави.
2. Це стан захисту об'єкта, за якого досягається його ефективна діяльність незалежно від ендогенних і екзогенних інформаційних впливів.
3. Це стан її захищеності, за якого сучасні інформаційні акти агресії не завдають шкоди національним інтересам.

У сучасних умовах інформаційна сфера вимагає прийняття адекватних заходів протидії ескалації іноземного інформаційного впливу в усіх його проявах. Шляхи вирішення даної проблеми полягають в наступних напрямах:

1. Систематичній діяльності з запобігань загрозам інформаційному простору, структуризація цілей та завдань з питань забезпечення інформаційної безпеки в фінансово-економічній сфері.
2. Активній протидії впливу на свідомість населення з метою зміни національних ідеологічних установок.
3. Розвитку вітчизняної технологічної та виробничої бази в галузі інформаційних технологій.
4. Підвищенні безпеки інформаційно-телекомунікаційних систем в сфері інформатизації озброєння та військової техніки.

5. Охорони державної таємниці, а також – іншої інформації з обмеженим доступом.

6. Вдосконаленні структури забезпечення інформаційної безпеки у сфері оборони [9, с. 744].

7. Захисті вітчизняного інформаційного простору від розповсюдження забороненої інформаційної продукції.

8. Обміні досвідом в інформаційно-комунікаційній галузі, а також підготовці кваліфікованих фахівців відповідно до вищих професійних стандартів.

Отже, підсумовуючи вищезазначене, інформаційна безпека – це здатність держави, суспільства та соціальних груп (групи) забезпечити інформаційні ресурси достатнім рівнем захищеності, надійності функціонування інформаційних та комунікаційних систем та протистояти інформаційним загрозам та небезпекам, негативним інформаційним впливам, підтримуючи постійну готовність до адекватних відповідей у інформаційному протиборстві.

Отже, є хороша думка, що проблеми інформаційної безпеки слід починати досліджувати з виявлення суб'єктів інформаційних відносин, їх інтересів, пов'язаних з використанням ІКТ, зворотною стороною яких є загрози інформаційній безпеці, а також правових інструментів держави.

Власне, його можна пов'язати з Інститутом секретності, а по-друге, його можна ототожнити з інформаційною (технологічною) сферою. На основі врахування національних інтересів в інформаційній сфері формуються стратегічні та поточні завдання внутрішньої і зовнішньої політики держави щодо забезпечення інформаційної безпеки.

Вона характеризується ступенем захищеності держави і суспільства, стабільністю основних сфер життєдіяльності (економіки, науки, техносфери, управління, військової справи, суспільної свідомості та ін.) по відношенню до

небезпечних дестабілізуючих деструктивних явищ, що робить негативний вплив на громадські та приватні інтереси.

Об'єктами небезпечного інформаційного впливу і, отже, інформаційної безпеки можуть бути визнані:

Ці інформаційні відносини породжуються інтересами суб'єктів, що реалізуються в інформаційній сфері.

На наш погляд, варто виділити наступні три основні групи цих інтересів::

- вільно володіє інформацією;

- передача окремих масивів інформації конкретним об'єктам;

- приховувати окремі масиви інформації від інших суб'єктів. Реалізуючи певні інтереси в інформаційній сфері, суб'єкт взаємодіє з іншими суб'єктами, певним чином оформляючи ці відносини, тобто дотримуючись певного порядку їх реалізації.

Цей правовий порядок залежить від рівня розвитку інформаційної інфраструктури, а також від засобів, якими суб'єкт може оперувати для реалізації своїх інтересів. У цивільно-правових відносинах відповідна взаємодія зазвичай приймає форму договору, об'єктом якого є послуга, а в суспільних відносинах-вимоги або звернення.

Давайте докладніше розглянемо можливі форми такої взаємодії. Взаємодія, пов'язана з пошуком інформації. Така взаємодія може відбуватися або у формі угоди, змістом якої є надання посередницьких послуг з пошуку повідомлень, що володіють необхідними особливостями (дизайн, зміст матеріальної або духовної сфери суспільства, рівень теоретичного узагальнення інформації, мова, якою представлені дані і т.д.), або шляхом надання суб'єкту взаємодії можливості самостійно вибирати потрібні йому повідомлення.

Соціальним результатом такої взаємодії може бути або визначення місця зберігання повідомлень, що відповідають характеристикам пошуку конкретного

суб'єкта, якому належать ці повідомлення, отримання дозволу на доступ до цих повідомлень, або відмова в наданні такого доступу суб'єкту або неможливість визначити місце зберігання бажаних повідомлень. Взаємодія, спрямована на отримання повідомлень, здійснюється у формі угоди, змістом якої є надання послуг з передачі необхідних повідомлень, а взаємодія, спрямована на зберігання повідомлень, - це Послуги із забезпечення збереження існуючих повідомлень. Соціальним результатом цих взаємодій буде отримання необхідних повідомлень, збереження фізичних властивостей матеріального носія, на якому вони закріплені, і, відповідно, можливість ознайомитися зі змістом цих повідомлень.

Взаємодія, спрямована на використання повідомлень для отримання інформації, здійснюється у формі угоди, зміст якої полягає в наданні можливості ознайомитися з важливими для суб'єкта повідомленнями.

Соціальним результатом цієї взаємодії є перетворення повідомлення в інформацію, яка відображається в "інформаційній моделі" суб'єкта. Взаємодія, спрямована на передачу (поширення) інформації, здійснюється у формі угоди, змістом якого є надання послуг з фіксації повідомлення, що містить ті інформацію, на матеріальному носії, а також передача (доведення) повідомлення певним суб'єктам або невизначеного числа суб'єктів певним способом (розсилка поштою, агітація і пропаганда, розміщення на рекламних щитах, поширення повідомлень в радіо-і телепрограмах, в інших засобах масової інформації, розміщення на сайтах тощо).

Соціальним результатом такої взаємодії є доставка повідомлення адресатам або ознайомлення адресатів з повідомленням, що за певних обставин може призвести до зміни їх поведінки. Взаємодія, спрямована на обробку інформації. Іноді фахівці виділяють інший тип інформаційних відносин-ті, які виникають в процесі взаємодії, спрямованого на обробку інформації.

Під обробкою інформації зазвичай розуміється перетворення певного набору повідомлень в нове повідомлення (набір повідомлень), яке здійснюється суб'єктом безпосередньо або технічними засобами, з використанням заздалегідь визначених алгоритмів або без них. Така взаємодія може здійснюватися у формі угоди, що полягає в наданні інформаційної (наукової, творчої) послуги, а його соціальним результатом є нове повідомлення або затвердження.

Взаємодія, спрямована на обробку інформації, можна розглядати як вид взаємодії, спрямованої на володіння інформацією, при якому частина операцій з підготовки повідомлень до сприйняття суб'єктами здійснюється з використанням комп'ютерних технологій.

У публічно-правових відносинах відбувається взаємодія для задоволення інтересів особистості і суспільства, пов'язаних з інформацією, що належить державі, а також інтересів держави, пов'язаних з інформацією, що належить фізичним особам і організаціям, органам місцевого самоврядування, що становить основу громадянського суспільства

Реалізація на практиці певних пріоритетів державної політики в інформаційній сфері вимагає великих зусиль уряду і матеріальних вкладень, яких сьогодні в державі недостатньо, що, в свою чергу, вимагає формування збалансованої державної політики та ефективної реалізації комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері, розробки механізму її реалізації.

Узагальнюючи підходи до розкриття змісту категорії "інформаційна безпека держави", можна визначити її основні особливості:

1.it є складовою частиною національної безпеки і стрімко розвивається як в Україні, так і в світі, Глобальна інформатизація охоплює всі сфери діяльності держави.

2.це стан захищеності об'єкта, при якому досягається його ефективна діяльність незалежно від ендогенних і екзогенних інформаційних впливів.

3.це стан її безпеки, при якому сучасні інформаційні акти агресії не завдають шкоди національним інтересам.

У сучасних умовах Інформаційна сфера вимагає вжиття адекватних заходів щодо протидії ескалації іноземного інформаційного впливу у всіх його проявах. Шляхи вирішення цієї проблеми лежать в наступних областях::

1. Системна діяльність щодо запобігання загроз інформаційному простору, структурування цілей і завдань щодо забезпечення інформаційної безпеки у фінансово-економічній сфері.

2. Активна протидія впливу на свідомість населення з метою зміни національних ідеологічних установок.

3. Розвиток вітчизняної технологічної та виробничої бази в галузі інформаційних технологій.

4. Підвищення безпеки інформаційно-телекомунікаційних систем в галузі інформатизації озброєння і військової техніки.

5. Захист державної таємниці, а також іншої інформації з обмеженим доступом.

6. Удосконалення структури забезпечення інформаційної безпеки у сфері оборони [9, с.744].

7. Захист вітчизняного інформаційного простору від поширення забороненої інформаційної продукції.

8. Обмін досвідом в інформаційно-комунікаційній галузі, а також підготовка кваліфікованих фахівців відповідно до найвищих професійних стандартів.

Отже, підводячи підсумок вищесказаному, інформаційна безпека-це здатність держави, суспільства і соціальних груп (груп) забезпечувати інформаційні ресурси достатнім рівнем безпеки, надійністю функціонування

інформаційно-комунікаційних систем і протистояти інформаційним загрозам і небезпекам, негативним інформаційним впливам, зберігаючи постійну готовність до адекватних дій у відповідь в інформаційному протистоянні.

Отже, є хороша думка, що проблеми інформаційної безпеки слід починати досліджувати з виявлення суб'єктів інформаційних відносин, їх інтересів, пов'язаних з використанням ІКТ, зворотною стороною яких є загрози інформаційній безпеці, а також правових інструментів держави.

Власне, його можна пов'язати з Інститутом секретності, а по-друге, його можна ототожнити з інформаційною (технологічною) сферою. На основі врахування національних інтересів в інформаційній сфері формуються стратегічні та поточні завдання внутрішньої і зовнішньої політики держави щодо забезпечення інформаційної безпеки.

Вона характеризується ступенем захищеності держави і суспільства, стабільністю основних сфер життєдіяльності (економіки, науки, техносфери, управління, військової справи, суспільної свідомості та ін.) по відношенню до небезпечних дестабілізуючих деструктивних явищ, що робить негативний вплив на громадські та приватні інтереси.

Об'єкти небезпечного інформаційного впливу і, отже, інформаційної безпеки можуть бути визнані об'єктами небезпечного інформаційного впливу:

1. свідомість, психіка людей;
2. інформаційно-технічні системи різного масштабу і призначення.

Якщо говорити про соціальні об'єкти інформаційної безпеки, то до них можна віднести індивіда, колектив, суспільство, держава і світове співтовариство. Що стосується суб'єктів інформаційної безпеки, то до них слід віднести ті органи і структури, які займаються її забезпеченням. Ми згодні з С. Домбровською в тому, що на практиці інформаційної безпеки взагалі не існує, незалежно від суб'єкта

інформаційного середовища, але саме суб'єкт диктує «параметри» такої безпеки [9].

Уважаємо, що її забезпечення в аспекті врахування інтересів суб'єкта інформаційних відносин представляє собою процес створення сприятливих умов діяльності, за яких реалізовувалися б його інтереси, здійснювалися б поставлені ним цілі.

1.2 Правові засади інформаційної безпеки

Базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України [1]. Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності [2]. Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації, встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

У ст. 1 закону інформація визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

Всі громадяни України, юридичні особи та державні органи мають право на інформацію, яка передбачає можливість вільного отримання, використання, поширення та зберігання інформації, необхідної їм для здійснення своїх прав, свобод і законних інтересів, виконання завдань і функцій. Кожному громадянину надається вільний доступ до інформації, що стосується його особисто, за винятком випадків, передбачених законодавством України. Розділ II Закону присвячений інформаційній діяльності, під якою розуміється сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Визначено основні напрями та види інформаційної діяльності – отримання, використання, поширення та зберігання інформації. Розділ III Закону визначає галузі, види, джерела інформації та спосіб доступу до неї. Основними галузями інформації є: політична, економічна, духовна, науково-технічна, соціальна, екологічна та міжнародна.

Основними видами інформації є: статистична; адміністративна інформація (дані); масова інформація; інформація про діяльність органів державної влади та органів місцевого та регіонального самоврядування; ПРАВОВА ІНФОРМАЦІЯ; Інформація про людину; інформація довідкового та енциклопедичного характеру; соціологічна інформація. Відповідно до режиму доступу інформація ділиться на відкриту інформацію та інформацію з обмеженим доступом. Держава контролює режим доступу до інформації. Державний контроль за дотриманням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України та Кабінет Міністрів України. Доступ до відкритої інформації забезпечується шляхом: систематичного опублікування її в офіційних друкованих виданнях (бюлетенях, збірниках); поширення її засобами масової інформації; безпосереднього надання її зацікавленим громадянам, державним органам та юридичним особам.

Обмеження права на отримання відкритої інформації заборонено законом. Інформація з обмеженим доступом ділиться на конфіденційну і секретну відповідно до її правовим режимом. Конфіденційна інформація - це інформація, яка знаходиться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюється за їх запитом відповідно до передбачених ними умов. Громадяни, юридичні особи, що володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, отриманої за свій рахунок, або такою, яка є предметом їх професійних, ділових, виробничих, банківських, комерційних та інших інтересів і не порушує передбачену законом таємницю, самостійно визначають режим доступу до неї, в тому числі її приналежність до категорії конфіденційної, і встановлюють систему (методи) її захисту. Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлюється Верховною Радою України за поданням Кабінету Міністрів України (за статистикою, екології, банківськими операціями, податками тощо), та інформація, приховування якої створює загрозу життю та здоров'ю людей.

До секретної інформації відносяться відомості, що містять відомості, що становлять державну та іншу встановлену законом таємницю (військову, комерційну, банківську, професійну, медичну, адвокатську таємницю і т.д.), розголошення яких завдає шкоди особистості, суспільству і державі. Інформація, що становить військову таємницю , - це вид секретної інформації, яка охоплює інформацію в галузі оборони, державної безпеки та правоохоронної діяльності, розголошення якої може завдати шкоди інтересам державної безпеки, боєготовності Збройних Сил України та інших військових формувань, їх окремих підрозділів, якщо ця інформація не належить до державної таємниці відповідно до законодавства України.

Інформація, що становить комерційну таємницю,- це інформація наукового, технічного, технічного, промислового, фінансово – економічного чи іншого характеру (в тому числі секрети виробництва-так звані ноу-хау), що має реальну або потенційну комерційну цінність в силу її незнання третім особам, до якої немає вільного доступу на законних підставах і щодо якої власником такої інформації введений режим комерційної таємниці. Порядок поширення секретної інформації, що не становить державну таємницю, та її захисту визначається відповідними державними органами за умови дотримання вимог Закону України"Про інформацію". Інформація з обмеженим доступом може поширюватися без згоди її власника, якщо вона є соціально значущою, тобто якщо вона є предметом суспільного інтересу і якщо право громадськості знати цю інформацію переважає над правом її власника на її захист.

Особливий вид секретної інформації-державна таємниця. Вона охоплює інформацію в галузі оборони, економіки, зовнішніх відносин, державної безпеки та правоохоронних органів, розголошення якої може завдати шкоди життєво важливим інтересам України і яка визначена в установленому законом порядку, є державною таємницею і підлягає державному захисту. Віднесення інформації до категорії відомостей, що становлять державну таємницю, порядок її захисту та розповсюдження, доступ до неї визначається законом України "Про державну таємницю", який закладає правові засади створення та функціонування системи захисту державної таємниці в Україні [3]. Ступінь секретності інформації визначається класифікацією секретності "таємно", "Цілком таємно"і" особливої важливості". Гриф видається на певний термін, який залежить від ступеня секретності: для грифа "таємно" – 5 років, "цілком таємно" – 10 років, "особливої важливості" – 30 років. Розділ IV Закону визначає учасників інформаційних відносин, їх права та обов'язки. Основними учасниками цих відносин є: автори, споживачі, розповсюджувачі, хранителі (хранителі) інформації.

Кожен учасник інформаційних відносин з метою забезпечення своїх прав, свобод і законних інтересів має право отримувати інформацію про: діяльність органів державної влади; діяльність народних депутатів; діяльність органів місцевого і регіонального самоврядування та місцевої адміністрації; про те, що стосується їх особисто. Розділ V Закону присвячений захисту інформації та відповідальності за порушення інформаційного законодавства. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації.

Стаття 45-1 забороняє цензуру і втручання в професійну діяльність журналістів і засобів масової інформації з боку державних органів або органів місцевого самоврядування та їх посадових осіб. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ненависті, посягання на права і свободи людини. Інформація, що стосується медичної таємниці, грошових внесків, комерційного прибутку, усиновлення, листування, телефонних розмов і телеграфних повідомлень, не підлягає розголошенню, за винятком випадків, передбачених законом. Порушення законодавства України Про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність відповідно до законодавства України. Розділ VI Закону присвячений міжнародній інформаційній діяльності, співпраці з іншими державами, іноземними та міжнародними організаціями в галузі інформації. Міжнародне співробітництво в галузі інформації з питань, що становлять взаємний інтерес, здійснюється на основі міжнародних угод, укладених Україною та юридичними особами, які здійснюють інформаційну діяльність.

Стаття 53 Закону визначає інформаційний суверенітет. Основою інформаційного суверенітету України є національні інформаційні ресурси.

Інформаційні ресурси України включають в себе всю інформацію, що належить їй, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами та міжнародними договорами.

Інформаційний суверенітет України забезпечений:

- виключне право власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету; - створення національних інформаційних систем;

- встановлення режиму доступу інших держав до інформаційних ресурсів України;

- використання інформаційних ресурсів на основі рівноправного співробітництва з іншими державами. Узагальнена класифікація інформації [4] відповідно до Закону України"Про інформацію".

Стаття 10 Закону України “Про засади національної безпеки України“ [5] визначає основні функції суб'єктів забезпечення національної безпеки України (Інформаційна сфера окремо не виділяється):

- розробка та періодичне уточнення Стратегії національної безпеки України та воєнної доктрини України, доктрин, концепцій, стратегій і програм, планування та реалізація конкретних заходів з протидії та нейтралізації загроз національним інтересам України;

- створення нормативної бази, необхідної для ефективного функціонування системи національної безпеки;

- удосконалення організаційної структури;

- Комплексне кадрове, фінансове, матеріально-технічне, інформаційне та інше життєзабезпечення компонентів (структурних елементів) системи;

- підготовка сил і засобів суб'єктів системи до їх використання відповідно до їх цільового призначення;

- постійний моніторинг впливу на національну безпеку процесів, що відбуваються в політичній, соціальній, економічній, екологічній, науково-технічній, інформаційній, військовій та інших сферах, релігійному середовищі, міжнаціональних відносинах; прогнозування змін, що відбуваються в них, і потенційних загроз національній безпеці;

- участь у двосторонньому і багатосторонньому співробітництві в галузі безпеки, якщо це відповідає національним інтересам України;

- спільне проведення планових та оперативних заходів у рамках міжнародних організацій та договорів у галузі безпеки.

Таким чином, створення необхідних правових та організаційних основ інформаційної безпеки було завершено. Основні принципи, норми та положення прийнятих законів та підзаконних актів відповідають загальноприйнятим міжнародно-правовим стандартам, в тому числі міжнародним конвенціям з прав людини.

Цими законами було закладено основні підвалини інформаційної безпеки України. Подальший розвиток цієї сфери державного будівництва вимагатиме удосконалення інфраструктури захисту інформації та законів і численних підзаконних актів та нормативних документів, якими регламентується діяльність цієї інфраструктури, а також діяльність органів державного управління, установ та організацій науки й виробництва, які використовують у своїй діяльності інформацію з обмеженим доступом.

На теперішній час в Україні розроблено основна правова та нормативна база, та створена інфраструктура, що має забезпечити надійний захист інформації у державі. Разом з тим слід пам’ятати, що технічні способи несанкціонованого зняття інформації та засоби протидії цим протиправним діям знаходяться у постійному розвитку. Зважаючи на цей безперервний розвиток та постійну інформаційну боротьбу, що складає один з важливих елементів сучасної світової

політики, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову інформаційної безпеки.

РОЗДІЛ 2. АНАЛІЗ ДЕРЖАВНОЇ ПОЛІТИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

2.1 Державна інформаційна політика України

Концепції Національної інформаційної політики України не випадково є визначення основних засад Національної інформаційної політики щодо побудови в Україні розвинутого інформаційного суспільства, забезпечення належних правових, економічних, внутрішньо- та зовнішньополітичних, організаційних та інших умов для його функціонування.

При аналізі політичних аспектів з державно-процесуальної точки зору інформаційна безпека може розглядатися в ряді областей, а саме: політичні інтереси, політичні відносини; у виборчих, державно-управлінських, зовнішньополітичних процесах і т. д. [11]. У той же час, за основними напрямками прояву, системний вираз інформаційної безпеки знаходить своє дихотомічне відображення в локалізації в наступних областях:

Таблиця 2.1

Аналіз основних напрямів прояву, системний вираз інформаційної безпеки України

№	Основними напрямками прояву, системний вираз інформаційної безпеки є:
1	у сфері функціонування державних органів політичної влади (Державна інформаційна безпека) [21];
2	у сфері громадянського суспільства (інформаційна безпека суспільства);
3	у сфері особистих інтересів [8, с.124].

Крім того, відповідно до рівнів соціальної організації та геополітичного змісту інформаційна безпека може бути забезпечена на міждержавному,

національному та внутрішньому рівнях (на рівні регіональних інститутів), а також на рівні органів місцевого самоврядування [9]. Інформаційна безпека-це результат інтеграції змісту понять" національна безпека "та" інформаційна безпека " [4].

Основними напрямками національної інформаційної політики України є: в галузі зв'язків з громадськістю:

1. забезпечення конституційних прав громадян на достовірну, повну та своєчасну інформацію, свободу слова та інформаційну діяльність у національному інформаційному просторі України, недопущення втручання у зміст та внутрішню організацію інформаційних процесів, за винятком випадків, визначених законом відповідно до Конституції України.

2. створення розвиненої інформаційно-комунікаційної інфраструктури для створення, збору, обробки, зберігання та використання національних інформаційних ресурсів.

3.збереження національного (національного) інформаційного продукту, національно-культурних і духовних цінностей України, її інформаційної та національно-культурної ідентифікації у світовому інформаційному просторі.

4. комплексна державна підтримка засобів масової інформації та забезпечення соціального та правового захисту журналістів та інших професійних творчих працівників, що займаються інформаційною діяльністю.

5.in виробнича сфера: збереження та ефективне використання державного і муніципального майна підприємств, інших об'єктів національного інформаційного простору України, визнаних об'єктами стратегічного значення в установленому законом порядку.

6. створення сприятливих умов для розвитку та захисту прав суб'єктів усіх форм власності на об'єкти національного інформаційного простору України та прав їх власників.

7. сприяння розвитку конкуренції.

8.Запобігання монополізації ринків у сфері інформаційної діяльності, в тому числі реклами.

9. економічна підтримка державою розвитку інформаційної інфраструктури та інформаційної системи України в цілому, незалежно від форм власності споруджуваних і розроблюваних об'єктів, сприяння в розробці та впровадженні новітніх інформаційних технологій..

10. підтримка вітчизняного виробника інформаційного продукту; в організаційній сфері: створення умов для своєчасного, якісного та ефективного інформаційного забезпечення громадян, органів державної влади, органів місцевого самоврядування, об'єднань громадян на основі національних інформаційних ресурсів.

11. адміністративний, технічний, судовий, міжнародно-правовий захист внутрішніх (національних) інформаційний продукт України, в цілому її інформаційні ресурси, особливо ті, які є національним надбанням України; дотримання принципів Європейської конвенції з прав людини, міжнародних документів у галузі міждержавного інформаційного співробітництва, ратифікованих Україною.

12. забезпечення ефективної присутності України у світовому інформаційному просторі шляхом розвитку транскордонного та прикордонного мовлення, поширення вітчизняної культурної, художньої та друкованої продукції у світі; у галузі науки, культури, підготовки кадрів та підвищення кваліфікації.

13.формування національної комп'ютерної мережі освіти, науки, культури, охорони здоров'я тощо в рамках глобального інформаційного простору..

14. послідовна реалізація заходів, спрямованих на підвищення кваліфікації, вдосконалення, використання та заохочення творчих кадрів в інформаційній сфері, захист авторських прав на інтелектуальну власність; демонополізацію інформаційних послуг і структур; створення комплексної системи збору, обробки,

створення і розповсюдження інформаційного продукту, який повинен задовольняти зростаючу потребу суспільства в інформації; вдосконалення засобів поширення інформації на основі новітніх технологій, зокрема впровадження волоконно-оптичних і супутникових каналів зв'язку.

15. створення мультимедійних систем і мереж, розширення можливостей медіаіндустрії; розвиток засобів масової інформації як найбільш ефективного джерела формування громадської думки; активне використання засобів масової інформації для обговорення соціально значущих нових ідей і проектів, адаптація населення до нових явищ суспільного життя..

16. підвищення ролі засобів масової інформації у формуванні позитивного іміджу України на міжнародному рівні.

Серед держав-членів ЄС розвиток інформаційного суспільства є одним із пріоритетних напрямів державної політики, що формально відображено в Європейській стратегії економічного зростання "Європа 2020: стратегія розумного, стійкого та всеохоплюючого зростання" (далі - "Європа 2020").

Серед семи стратегічних напрямків, викладених у цьому документі, окремою програмою є " цифровий Порядок денний для Європи "(Digital Agenda for Europe), яка замінила попередню європейську програму "2014 - Європейське інформаційне суспільство для зростання та зайнятості".

Сім напрямків роботи, намічених у програмі "Європа 2020", є пріоритетними як для Європейського Союзу в цілому, так і для країн-учасниць. Для усунення перешкод і досягнення стратегічних цілей використовується ряд політичних, економічних і соціальних інструментів. В першу чергу це стосується внутрішнього ринку, фінансових механізмів, інструментів зовнішньополітичної діяльності.

Механізми реалізації "Європа 2020" і такий компонент, як" Цифровий порядок денний", передбачають, що будуть розроблені єдині керівні принципи для

кожного напрямку роботи та рекомендації для європейських держав, будуть впроваджені засоби впливу в умовах, коли країна-учасниця не зможе адекватно реагувати на ситуацію, будуть представлені звіти про те, як реалізується ця стратегія, де буде оцінена її ефективність і чітко визначені основні діючі особи, коло їх завдань і функцій.

Цей підхід, заснований на співпраці між владою ЄС, носить однаковий характер і використовується в діяльності комітетів, національних парламентів, національних, регіональних і місцевих органів влади, громадських сил і громадянського суспільства в цілому.

Україна, яка має намір отримати статус асоційованого члена Європейського Союзу, повинна враховувати такі механізми і здійснювати максимальну адаптацію існуючих національних механізмів в рамках міжнародної угоди "Порядок денний асоціації Україна - ЄС".

Інформаційна безпека є невід'ємною частиною національної безпеки і розглядається як пріоритетна функція держави.

Інформаційна безпека, з одного боку, передбачає забезпечення якісної всебічної інформації громадян і вільного доступу до різних джерел інформації, а з іншого - це контроль за запобіганням поширення дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам і захист національного інформаційного простору від маніпуляцій, інформаційних воєн і операцій.

Вирішення комплексної проблеми інформаційної безпеки дозволить як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації [59].

Протидія зовнішнім загрозам інформаційній безпеці України відбувається в контексті прогресивної тенденції до переформатування сфер впливу в

глобальному просторі на тлі глобалізації політичних, соціально-економічних і культурних відносин.

Виявлення та аналіз відповідних загроз ускладнюється низкою факторів: частина населення вважає, що зовнішніх загроз для країни Немає; Військова доктрина і доктрина інформаційної безпеки не дають чіткого визначення потенційних зовнішніх загроз для країни, що призводить до відсутності чіткої класифікації і ранжирування загроз за ступенем значущості і порівняльній динаміці їх збільшення; відсутності чіткого розуміння причин і джерел цих загроз і т.д. [42].

Як зазначається, рівень розвитку та захищеності інформаційного середовища, які є одними з найбільш значущих факторів у всіх сферах державної безпеки, активно впливають на стан політичної, економічної та інших складових державної безпеки в Україні. У зв'язку з цим доцільно розглядати інформаційну безпеку як складову інших сфер державної безпеки. Водночас інформаційна безпека є самостійною складовою державної безпеки, і це свідчить про її двоїсту природу.Це пов'язано з наступним:

1. Прагнення кожної держави реалізувати і захистити власні національні інтереси, які спрямовані на формування і накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів.

2. Необхідність не тільки розвитку і зміцнення національного інформаційного потенціалу, а й захисту від широкого спектру існуючих і потенційних інформаційних загроз.

3. Існує реальна необхідність захисту всіх суб'єктів інформаційних відносин від можливих негативних наслідків впровадження та використання інформаційних технологій.

4. Існуюча можливість інформаційного тиску на Україну, навіть інформаційної агресії з боку розвинутих країн світу з метою отримання односторонніх переваг у політичній, економічній, військовій та інших сферах, а також інформаційного впливу на свідомість і підсвідомість окремих осіб, сім'ю, суспільство і держава, що загрожує державній безпеці [7].

Державна політика інформатизації отримала новий імпульс лише останнім часом у зв'язку з усвідомленням необхідності побудови в Росії інформаційного суспільства як головної умови її політичного і соціально-економічного розвитку і збереження статусу світової держави.

Вирішення цього важливого завдання сприяло переходу від політики інформатизації до інформаційної політики, що включає геополітичні, зовнішньоекономічні, соціально-економічні, науково-технічні та культурні аспекти розвитку країни.

В рамках Державної інформаційної політики мають бути закладені основи для вирішення таких завдань, як формування єдиного інформаційного простору та його входження у світовий інформаційний простір, забезпечення інформаційної безпеки особистості, суспільства і держави, формування демократично орієнтованої масової свідомості, формування індустрії інформаційних послуг, розширення правової бази регулювання суспільних відносин, у тому числі пов'язаних з отриманням, поширенням і використанням інформації.

Державна інформаційна політика повинна служити інструментом зміцнення зв'язку між Центром і регіонами, забезпечення реалізації єдиної державної політики на всій території країни.

Необхідність вирішення таких масштабних завдань потребує управління всіма видами інформаційних ресурсів, елементами інформаційно-телекомунікаційної інфраструктури, державної підтримки вітчизняного інформаційного виробництва, ринку інформаційних технологій, засобів, продуктів

і послуг, регулювання діяльності державних електронних та друкованих засобів масової інформації.

Процеси формування та розвитку світової інформаційної спільноти та рух розвинених країн від індустріального до постіндустріального (інформаційного) суспільства мають виняткове значення для розвитку відповідних уявлень про інформатизацію, політику інформатизації та державну інформаційну політику в цілому.

Цей рух спирається на новітні інформаційні, телекомунікаційні та комунікаційні технології.

Саме нові технології призвели до швидкого поширення глобальних інформаційних мереж, в першу чергу Інтернету, що відкриває принципово нові можливості для міжнародного обміну інформацією.

Перспективні інформаційні та телекомунікаційні технології багаторазово посилюють вплив електронних засобів масової інформації на суспільно-політичне та культурне життя мільйонів людей на всіх континентах. Цей рух концептуально і практично визначає формування глобального інформаційного простору.

Таким чином, державна інформаційна політика повинна стимулювати зростання виробництва засобів інформатизації, телекомунікацій, інформаційних продуктів і послуг і в той же час платоспроможного попиту на них.

У той же час практична реалізація державної інформаційної політики в сучасних умовах суспільного розвитку вимагає широкої психологічної кампанії з підтримки її основних положень у громадській думці, роз'яснення її соціальної спрямованості, доказу її обґрунтованості і так далі.

Указ президента України № 96 від 15 березня 2016 року "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"".

Доктрина інформаційної безпеки України (далі-доктрина) визначає національні інтереси держави в інформаційній сфері, загрози їх реалізації, напрями та пріоритети державної політики в інформаційній сфері.

Правовою основою доктрини є Конституція України, закони України, стратегія національної безпеки України, затверджена Указом Президента України № 287 від 26 травня 2015 року "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про стратегію національної безпеки України", а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України [2].

Поряд з національними інтересами України в інформаційній сфері доктрина визначає актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері, а саме:

1.здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань.

2.провокування екстремістських проявів; підживлення панічних настроїв.

3.загострення і дестабілізація суспільно-політичної та соціально-економічної ситуації.

4.розпалювання міжнаціональних і міжконфесійних конфліктів в Україні.

5. проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі; інформаційна експансія держави-агресора та підконтрольних їй структур, у тому числі шляхом розширення власної інформаційної інфраструктури на території України та в інших державах.

6.інформаційне домінування держави-агресора на тимчасово окупованих територіях.

7.недостатній розвиток національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та активно діяти в інформаційній сфері для реалізації національних інтересів України.

8.неефективність державної інформаційної політики.

9.недосконаліть законодавства про регулювання суспільних відносин в інформаційній сфері; невизначеність стратегічного наративу.

10. недостатній рівень медіакультури суспільства; поширення закликів до радикальних дій.

11.пропаганда ізоляціоністських і автономістських концепцій регіонального співіснування в Україні [3].

Основним органом з реалізації заходів інформаційної безпеки держави є Рада національної безпеки і оборони України, яка відповідно до Конституції України та в установленому законом порядку має координувати діяльність органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. Центральним органом виконавчої влади є Кабінет Міністрів України, який повинен забезпечувати реалізацію державної інформаційної політики, фінансувати програми, пов'язані з інформаційною безпекою, направляти і координувати роботу міністерств та інших органів виконавчої влади у цій сфері.

Не менш важливі функції з реалізації завдань, поставлених при реалізації Основних положень доктрини в галузі інформаційної безпеки, виконує Міністерство інформаційної політики України, на яке в установленому порядку покладено:

1. Організація та забезпечення моніторингу засобів масової інформації та загальнодоступних ресурсів вітчизняного сегменту мережі Інтернет з метою виявлення інформації, поширення якої в Україні заборонено.

2. організація та забезпечення моніторингу загроз національним інтересам та національній безпеці в інформаційній сфері.

3. сприяння Міністерству закордонних справ України у доведенні офіційної позиції України до іноземних засобів масової інформації.

4.формування поточних пріоритетів державної інформаційної політики, контроль за їх реалізацією.

5. Координація діяльності центральних та місцевих органів виконавчої влади в галузі забезпечення інформаційного суверенітету України, урядового зв'язку, кризового зв'язку, в тому числі в період проведення антитерористичної операції та в особливий період.

6.вжиття заходів в інформаційній сфері, пов'язаних з введенням правових режимів надзвичайного або воєнного стану.

7.розробка стратегічного наративу та його реалізація.

8.Розробка та реалізація стратегії інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій.

9.Розробка та впровадження єдиних стандартів підготовки фахівців у галузі урядового зв'язку для потреб державних органів [3].

Певні завдання покладено на Міністерство закордонних справ України, Міністерство оборони України, Міністерство культури України, Державне агентство України з питань кіно, Національну Раду України з питань телебачення і радіомовлення, Державний комітет України з питань телебачення і радіомовлення, Службу безпеки України, спецслужби України, Державну службу спеціального зв'язку та захисту інформації України, Національний інститут стратегічних досліджень та ін.

Отже, ефективна реалізація стратегічних пріоритетів, основних принципів і завдань державної політики інформаційної безпеки потребує вдосконалення правових і організаційних механізмів управління інформаційною безпекою, її

відповідного інтелектуально-кадрового і ресурсного забезпечення, зокрема й вдосконалення законодавства з питань національної безпеки, насамперед, шляхом: розвитку правових засад управління національною безпекою через розроблення відповідних законів, концепцій, доктрин, стратегій і програм, зокрема й антикорупційного законодавства, Національної програми протидії тероризму й екстремізму, Концепції розвитку Воєнної організації держави, Національної стратегії формування інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо; розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами, зокрема і з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність; узгодження законодавства з питань охорони державної таємниці з європейськими стандартами; розроблення та впровадження загальнодержавної системи визначення і моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці [4].

Отже, у сучасних умовах важливим складником національної безпеки є інформаційна безпека України, що є станом захищеності національних інтересів в інформаційній сфері.

На нашу думку, для захисту та посилення інформаційної безпеки варто розвивати вітчизняну індустрію інформації відповідно до сучасної геополітичної ситуації у світі; розробляти програмні й апаратні засоби криптографічного захисту інформації, які б захищали інформаційні ресурси від несанкціонованого доступу для забезпечення конфіденційності; запровадити ліцензування та розробити критерії сертифікації технологій; здійснювати інформатизацію й автоматизацію виробничих процесів і робочих місць співробітників.

Зважаючи на плани підвищення інформаційної безпеки держави, головним завданням державної політики в зазначеній сфері має стати оптимізація діяльності самої влади, її структури, підвищення оперативності й якості рішень, ефективне використання бюджетних витрат і утримання владної структури та сукупних непродуктивних витрат часу та коштів під час взаємодії влади, населення та бізнесу. Становлення інформаційного суспільства в Україні обумовило прискорення темпів розвитку мережі Інтернет. За останні роки кількість користувачів Інтернет в Україні значно зросла. Це свідчить про те, що дедалі більше громадян стає активними учасниками інформаційних відносин.

Інтенсивність розширення аудиторії споживачів інформації спонукає до вирішення найбільш гострих проблем сучасності: забезпечення конструктивного і безпечного використання національного інформаційного простору, розробки і реалізації комплексу політичних, правових, економічних, соціально-культурних та організаційних заходів держави, спрямованих на забезпечення конституційного права громадян на доступ до інформації, тобто формування державної інформаційної політики, яка б повною мірою відповідала сучасним реаліям.

Сьогодні в Україні сформульовано й законодавчо закріплено основні принципи, завдання та стратегічні напрями державної інформаційної політики, сформовано державні інститути відповідної компетенції, ухвалено цілу низку концепцій, програм і планів дій.

Проте, інформаційна політика держави характеризується різноспрямованістю, нескоординованістю діяльностірізних відомств, непослідовністю та непрозорістю вреалізації запланованих заходів. Зважаючи на ці обставини, Україну не можна віднести до інформаційно незалежних держав.

Сьогодні державна інформаційна політика спрямована на розбудову якісно нового вітчизняного інформаційного суспільства, що є запорукою політичного і

соціально-економічного руху України вперед, зміцнення її статусу, як незалежної держави [1].

Значна кількість питань, пов'язаних з розвитком інформаційного суспільства, досі не вирішені на законодавчому рівні. Це стосується, зокрема, інфраструктурних проблем, діяльності ЗМІ, інформаційно - аналітичних інститутів і так далі.

Істотним недоліком чинного інформаційного законодавства є те, що воно носить занадто загальний характер, не визначає шляхів вирішення проблем, що виникають при використанні інформаційного простору. Концептуальна основа також залишається недосконалою, що істотно ускладнює реалізацію завдань і взаємодію суб'єктів інформаційної сфери.

В Україні відсутнє правове регулювання функціонування міжнародних інформаційних систем, однією з яких є Інтернет. Продовжує зберігатися неповнота правового регулювання питань інформаційної безпеки, що, в свою чергу, створює нові виклики і загрози національній безпеці України.

Ситуація особливо загострюється при міжнародному обміні інформацією через глобальні соціальні мережі, що посилює вплив електронних та друкованих ЗМІ на суспільно-політичне та культурне життя країни, моральний стан суспільства тощо [22].

Вкрай важливо створити основу для формування стабільного та безпечного інформаційного простору в Україні, а також необхідні умови для її інтеграції у світовий інформаційний простір.

Держава повинна здійснювати заходи щодо забезпечення інформаційної безпеки особистості, суспільства і держави, приділяти увагу значному розширенню переліку вітчизняних інформаційних послуг для населення, забезпечувати правове регулювання відносин у національній інформаційній сфері.

У рамках державної інформаційної політики важливо акцентувати увагу на формуванні таких загальнообов'язкових норм поведінки користувачів, як інформаційна культура та відповідальне ставлення до використання інформаційного простору.

Реалізація цих завдань передбачає вдосконалення системи управління всіма видами інформаційних ресурсів та інформаційно-телекомунікаційною інфраструктурою, забезпечення державної підтримки процесу формування ринку інформаційних технологій, інструментів і продуктів.

Форми та напрями співпраці держави з електронними та друкованими ЗМІ потребують подальшого вдосконалення. Метою державної інформаційної політики має стати побудова в країні демократичного інформаційного суспільства, інтегрованого у світове інформаційне співтовариство.

Для досягнення цієї мети необхідно зосередити зусилля на створенні необхідних умов і механізмів, спрямованих на створення, розвиток і забезпечення ефективного використання інформаційних ресурсів у всіх сферах діяльності.

Серед пріоритетних завдань державної інформаційної політики слід виділити створення сприятливих умов для формування, розвитку, модернізації та використання національних інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури та технологій [12].

Цьому повинен передувати детальний аналіз існуючої нормативної бази та визначення шляхів і напрямків її вдосконалення з урахуванням сучасних реалій. Необхідно окреслити основні принципи та механізми обліку інформаційних ресурсів, створених за рахунок коштів державного бюджету, а також критерії об'єктивної оцінки їх якості та можливостей.

Слід також подбати про реформування інформаційного забезпечення в системі органів державної влади. Інформаційна політика держави повинна

сприяти розвитку внутрішнього ринку інформаційно-телекомунікаційних систем і технологій, орієнтованих на роботу у внутрішніх комп'ютерних мережах.

Для цього необхідно вдосконалювати механізми і вишукувати ресурси для надання державної підтримки перспективним вітчизняним дослідженням, спрямованим на створення власних інформаційно-телекомунікаційних систем і технологій.

Особливу увагу слід приділити вдосконаленню практики виявлення перспективних наукових розробок з метою їх подальшого фінансування з бюджету та забезпечення мінімального впливу людського фактору на прийняття таких рішень.

Важливе місце в державній Інформаційній Політиці має відводитися нормативному регулюванню функціонування міжнародних інформаційних систем в Україні, а також електронних і друкованих засобів масової інформації.

Необхідно забезпечити вільне поширення інформації та конституційне право громадян на її Пошук, отримання, виробництво і поширення. Особливу увагу слід приділити розвитку співпраці держави із засобами масової інформації, оскільки засоби масової інформації часто є основними джерелами інформації і відіграють роль важливого соціального інституту в реалізації державної інформаційної політики.

Назріла гостра необхідність у розробці правових, економічних і організаційних механізмів забезпечення балансу інтересів особистості і держави в діяльності засобів масової інформації, недопущення їх монополізації, сприяння ефективному виконанню функції об'єктивного і неупередженого інформування суспільства про події внутрішнього і міжнародного життя.

Також необхідно врегулювати проблеми, пов'язані з доступом до інформації журналістів, правовим захистом особистої таємниці в засобах масової інформації, захистом громадян і суспільства від неправдивої і недобросовісної інформації.

У процесі формування та вдосконалення інформаційної політики держави необхідно на законодавчому рівні виключити підпорядкування засобів масової інформації будь-яким кон'юнктурним інтересам, вжити заходів щодо недопущення спроб чинення на них тиску, а також спроб надання суб'єктами інформаційних відносин неповної, спотвореної або недостовірної інформації для засобів масової інформації.

Варто зазначити, що проблема визначення принципів протидії зовнішньому впливу на внутрішньополітичну ситуацію в Україні в рамках державної інформаційної політики стає все більш актуальною.

Сьогодні існує необхідність посилення державного контролю за діяльністю міжнародних неурядових організацій, що існують за рахунок коштів і ресурсів, у тому числі фінансових, що надаються іноземними урядами або їх структурами [22].

Протягом усіх років незалежності, в умовах динамічного розвитку міжнародної політичної ситуації і загострення конкуренції між провідними центрами сили за посилення їх глобального та регіонального впливу, однією з найбільш істотних загроз національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу, шляхом проведення Інформаційних акцій, Операцій, Кампаній.

Іноземні суб'єкти інформаційних відносин часто чинять потужний негативний інформаційно-психологічний вплив на Україну, поширюючи необ'єктивну, неповну або необ'єктивну інформацію.

Варто зазначити, що інтенсивність такого впливу значною мірою не залежить від політичних сил, які перебувають при владі в Україні, а зумовлена в першу чергу прагненням керівництва іноземних держав впливати на зовнішню і внутрішню політику нашої держави, а також має політичну та економічну основу,

продиктовану прагматичними підходами до забезпечення власних національних інтересів[4].

За характером зовнішнього інформаційно-психологічного впливу на Україну іноземні держави можна розділити на дві групи: групу ситуаційного впливу і групу постійного впливу.

До групи ситуаційного впливу входить більшість західних держав, інформаційні впливи яких на Україну в основному стосуються перспектив європейської інтеграції України, внутрішньополітичної та економічної ситуації в нашій державі, російсько-українських відносин, деяких аспектів інтерпретації історії і так далі. До країн, що надають постійний і найбільш інтенсивний інформаційно-психологічний вплив на Україну, слід віднести, перш за все, Російську Федерацію (про що особливо яскраво свідчать події початку березня 2017 року і загострення українсько-російських відносин) [25], А також Румунію та Угорщину.

Удосконалення правового забезпечення державної інформаційної політики передбачає формування нормативної бази, спрямованої на регулювання інформаційних відносин у суспільстві, забезпечення рівності всіх учасників інформаційної взаємодії та контроль за додержанням законодавства у цій сфері.

Важливою проблемою залишається певна неузгодженість державної правової політики в інформаційній сфері, зокрема, у зв'язку з тим, що в основному законодавчі акти приймаються для вирішення тактичних завдань без урахування стратегічних орієнтирів та об'єктивних умов України.

Крім того, деякі інформаційні відносини регулюються підзаконними актами, а іноді і відомчими нормативними актами [16]. Необхідно уточнити перелік підстав для обмеження доступу до інформації та визначення персональної відповідальності посадових осіб і посадових осіб як за розголошення конфіденційної, так і за обмеження доступу до відкритої інформації.

Необхідно передбачити шляхи і механізми захисту суспільства від неправдивої, спотвореної або недостовірної інформації, отриманої через засоби масової інформації.

Відповідальність за порушення в інформаційній сфері також повинна регулюватися законом.

Варто зазначити, що нормативна база в галузі регулювання розвитку інформаційного суспільства та заходи з формування державної інформаційної політики повинні повністю відповідати завданням в галузі інформаційної безпеки, практиці забезпечення збереження державної таємниці, захисту інформаційно-телекомунікаційної інфраструктури та інформаційних ресурсів від кібератак та інших загроз в інформаційному просторі.

Важливо створити сприятливі умови для вдосконалення вітчизняних систем захисту інформації, що стає особливо актуальним у зв'язку з розширенням обміну інформацією через Інтернет. Існує нагальна необхідність у розробці узгоджених правил і процедур захисту національних інтересів України в процесі інтеграції в міжнародні інформаційні мережі.

Враховуючи, що державна інформаційна політика має суттєвий вплив на різні аспекти суспільного життя, необхідне впровадження ефективної системи своєчасного виявлення та протидії небезпеці використання нових інформаційних технологій для створення реальних та потенційних загроз національній безпеці України [7].

Стратегія розвитку інформаційного суспільства України повинна передбачати активну співпрацю в цій сфері з іншими державами.

Доцільно реалізувати комплекс заходів, спрямованих на забезпечення інтересів країни в міжнародному інформаційному обміні та забезпечення безпеки Національних інформаційних ресурсів та інформаційно-телекомунікаційної інфраструктури.

Державна інформаційна політика повинна закласти основи для вирішення фундаментальних проблем розвитку суспільства, основними з яких є формування єдиного інформаційного простору України та її входження у світовий інформаційний простір, забезпечення інформаційної безпеки особистості, суспільства і держави.

Крім того, велику увагу слід приділити формуванню демократично орієнтованої масової свідомості, формуванню індустрії інформаційних послуг, законодавчому регулюванню суспільних відносин, в тому числі пов'язаних з отриманням, поширенням і використанням інформації.

В умовах мінливості і суперечливості глобального простору, проникнення кордонів і формування нової політичної географії між окремими державами і регіонами виникли нові протиріччя різного типу.

Політичні, економічні, конфесійні, етнічні та інші протиріччя, спроби перегляду існуючих кордонів і перерозподілу сфер впливу призвели до низки гострих конфліктів. У протиріччях між державами засоби і можливості інформаційної війни широко використовуються для досягнення успіху, тобто використання і управління інформацією з метою отримання конкурентної переваги над противником.

У контексті неоголошеної російсько-української війни на Донбасі та окупації Криму та частини Донецької та Луганської областей засоби такої війни широко використовувалися Росією в Україні. Тому забезпечення інформаційної безпеки стало важливим завданням для України.

Стаття 17 Конституції України свідчить, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу [7].

Тому інформаційну безпеку слід розглядати як ефективну протидію зовнішнім і внутрішнім загрозам з метою забезпечення інформаційного суверенітету.

Водночас під інформаційним суверенітетом держави на законодавчому рівні розуміється здатність держави контролювати і регулювати потік інформації з-за меж держави з метою дотримання законів України, прав і свобод громадян та забезпечення національної безпеки держави [13].

Інформаційна безпека розглядається поряд з кібербезпекою, захистом персональних даних, недоторканністю приватного життя і правами цифрових користувачів, зміцнення і захист довіри в кіберпросторі визначається передумовою одночасного цифрового розвитку і належного запобігання, усунення та управління пов'язаними з цим ризиками.

Інформаційна безпека також розкрита в доктрині інформаційної безпеки України від 25 лютого 2017 року [11] як невід'ємна складова кожної зі сфер національної безпеки і як важлива самостійна сфера забезпечення національної безпеки.

Забезпечення інформаційної безпеки є невід'ємним процесом впровадження системи національної безпеки .

Основними функціями системи інформаційної безпеки є:

- Превентивна: реалізація комплексу заходів, спрямованих на запобігання та нейтралізацію загроз;

- прогнозування: прогнозування та виявлення внутрішніх і зовнішніх загроз;

- управління: створення умов і можливостей для ефективного управління інформаційними ресурсами.

Інформаційна безпека держави багато в чому залежить від загальної фінансово-економічної ситуації і політики, що проводиться в державі.

Серед завдань, які повинні виконуватися суб'єктами системи інформаційної безпеки, слід виділити наступні::

- виявлення факторів, ризиків та загроз інформаційній безпеці;

- визначення показників інформаційної безпеки та порівняння їх з граничними;

- розробка системи моніторингу, яка включатиме моніторинг, збір, обробку, зберігання та аналіз інформації про стан інформаційної безпеки держави;

- розробка заходів, спрямованих на зміцнення інформаційної безпеки держави.

Щодо визначення існуючих основних загроз національним інтересам та національній безпеці України, серед яких є й інформаційні загрози, законодавець виділив ці фактори у статті 7 Закону України "Про засади національної безпеки України".

Їх перелік наведено в цій статті за дев'ятьма напрямками суспільних відносин: внутрішня, зовнішня політика, військова, безпека, економічна, науково-технічна, Цивільний захист, Екологічна, Інформаційна. Конкретизуючи останній напрямок, законодавець відзначає наступні загрози в інформаційній сфері::

1. прояви обмежень свободи слова та доступу до публічної інформації.

2.поширення в засобах масової інформації культу насильства, жорстокості, порнографії.

3. комп'ютерна злочинність і комп'ютерний тероризм.

4.розголошення відомостей, що становлять державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави.

5.спроби маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [23].

Враховуючи, що даний закон був істотно змінений в 2014-2015 роках і заснований на переліку цих загроз в інформаційній сфері, слід зазначити, що в ньому відсутня велика кількість важливих елементів цих загроз і не відображений їх повний перелік.

Всього через два роки після внесення змін в закон України "Про основи національної безпеки України", рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року "Про доктрину інформаційної безпеки України", яке було введено в дію Указом Президента України від 25 лютого 2017 року № 47/2017, основні джерела загроз інформаційній безпеці України були розділені відповідно до статті 7 закону України "Про основи національної безпеки України" на внутрішні і зовнішні.

До зовнішніх загроз відносяться:

- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та підконтрольних йому структур, зокрема шляхом розширення власної інформаційної інфраструктури на території інших держав.

Внутрішні загрози включають:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, розпалювання панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжнаціональних і міжконфесійних конфліктів в Україні;

- інформаційна експансія держави-агресора та підконтрольних йому структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України;

- інформаційне домінування держави-агресора на тимчасово окупованих територіях;

- недостатній розвиток національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та активно діяти в інформаційній сфері для реалізації національних інтересів України;

- неефективність державної інформаційної політики, недосконаліть законодавства про регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських і автономістських концепцій регіонального співіснування в Україні [4].

Так, аналізуючи наведений вище перелік інформаційних загроз, визначений рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року "про доктрину інформаційної безпеки України", слід зазначити, що в Раді національної безпеки і оборони України вказані внутрішні та зовнішні загрози інформаційній безпеці України, відображено повний перелік їх основних складових в умовах сучасної інформаційної війни. Крім того, в доктрині визначено пріоритети державної політики в інформаційній сфері, а також механізм її реалізації.

Неможливо не помітити, що у сучасному суспільстві інформація набуває все більш важливої ролі. І це змінює правила гри у військовій, політичній та економічній сферах.

Новий інструментарій в арсеналі інформаційного протиборства привносить не лише значно дешевші засоби впливу, які досить часто навіть помітити складно, що несе в собі приховану небезпеку, яку необхідно вчасно виявляти та нейтралізовувати в найкоротший термін [5].

В той же час слід відмітити що визначення і конкретизація зазначених загроз, пріоритети державної політики у цій сфері та механізм протидії визначався достатньо повільно, оскільки з початку окупації Російською Федерацією Кримського півострову та гібридної війни проти України на Донбасі пройшло майже три роки, внаслідок чого наша держава зазнала великих людських, територіальних, фінансових втрат.

Перш за все слід відзначити, що тимчасова втрата частини території України стала можливою за рахунок успішного ведення інформаційної війни проти України, а саме внаслідок проведення низки руйнівних інформаційних операцій на нашій території, поєднаних з військовими діями, націленими на позбавлення нашої країни територіальної цілісності.

До основних перешкод на шляху побудови ефективної системи інформаційної безпеки України слід віднести недостатнє фінансування та низькій рівень технічного забезпечення спеціально уповноважених органів державної влади у цій сфері, недостатня кількість кваліфікованих кадрів, незадовільний рівень оплати праці фахівців цього напрямку, низький рівень координації органів державної влади з суміжними повноваженнями, ускладнений порядок обміну інформацією внаслідок недосконалого законодавчого регулювання.

Відповідно до вищенаведеного, задля вдосконалення системи інформаційної безпеки державою повинні бути зроблені певні кроки у цьому напрямі, а саме: здійснення підвищення фінансування та збільшення рівня технічного забезпечення уповноважених державних органів у сфері інформаційної безпеки держави, запровадити та інтенсифікувати існуючі програми навчання та обміну досвідом з відповідними компетентними державними органами країн ЄС та НАТО в сфері інформаційної безпеки, ведення уповноваженими органами та посадовими особами переговорів щодо вирішення питання про надання Україні допомоги в рамках міжнародних програм у галузі інформаційно-технічного співробітництва.

Вирішення державою вищезазначених проблем значно підвищить рівень інформаційної захищеності України та позитивно вплине на загальний рівень стану безпеки.

Таким чином, врахування вище зазначених проблем при визначенні основних засад формування і реалізації державної інформаційної політики сприятиме посиленню безпеки держави в політичній, економічній та соціальній сферах, стане дієвим засобом протидії загрозам національної безпеки України.

2.2 Сутність, рекомендації та преспективи державної політики в сфері інформаційної безпеки України

З метою протидії негативним впливам інформаційної пропаганди та інформаційних війн, задля нейтралізації та упередження реальних та потенційних загроз в інформаційному просторі України, Рада національної безпеки і оборони України ухвалила рішення “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України”.

У документі зазначено, що РНБО, враховуючи необхідність вдосконалення нормативно-правового забезпечення та запобіганняння й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, в и р і ш и л а : розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема забороною ретрансляції телевізійних каналів; посилити контроль за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки; ужити заходів щодо забезпечення поширення у світі об’єктивних відомостей про

суспільно-політичну ситуацію в Україні, зокрема, через створення відповідного медіахолдингу для підготовки якісного конкурентоздатного інформаційного продукту; розробити порядок аналізу інформаційних матеріалів іноземних ЗМІ, що мають представництва в Україні, з метою впровадження дієвого механізму акредитації журналістів; ужити заходів до активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності [15].

Крім вищезазначеного документа, основні напрями державної політики з питань національної безпеки в інформаційній сфері визначені у Законах України "Про основи національної безпеки України", "Про Основні засади розвитку інформаційного суспільства в Україні у "Доктрині національної безпеки" та в інших нормативно-правових документах. Отже, в умовах сучасних інформаційних протистоянь, експансіоністської політики Російської федерації, національний інформаційний простір України є недостатньо захищеним від зовнішніх негативних пропагандистських інформаційно-психологічних впливів, загроз.

Тому захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки України, розроблення дієвих стратегій і тактик протидії медіазагрозам повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів. Актуальність досліджуваної у роботі проблематики – незаперечна і потребує поглибленого вивчення.

Перспективами подальших наукових досліджень є: аналіз зарубіжного досвіду протидії негативним пропагандистсько-маніпулятивним інформаційним впливам, а також глибше дослідження технологій здійснення інформаційних операцій та війн.

ВИСНОВКИ

У роботі було встановлено:

1. З’ясовано зміст інформаційної безпеки, який правомірно розглядати в межах дихотомічності інформаційної сфери, елементами якої визнано сукупність інформації, засобів її виробництва, обробка та зберігання, інформаційний простір й інфраструктура, суб'єктів, що здійснюють збір, формування, розповсюдження і використання інформації, а також системи державного управління, виникаючих при цьому державно-владних відносин. Така система передбачає здійснення цілеспрямованого й організуючого впливу керованої підсистеми (держави) на сферу інформаційної безпеки шляхом застосування правового й організаційного інструментарію, який становить підґрунтя для класифікації механізмів державної політики в означеній сфері.

2. Під час аналізу дії правового й організаційного механізмів державної політики у сфері інформаційної безпеки в Україні встановлено таке:

- відсутня єдина інфраструктура зв'язку й інформації державних органів влади, побудована на єдиних стандартах і платформах, ускладнюючи тим самим процес своєчасного впровадження сучасних технологій;
- діючі інформаційні системи органів державної влади були розроблені і введені в експлуатацію в різний час, що й зумовило несумісність програмнотехнічних рішень сьогодні;
- вітчизняна правова база відзначається розпорошенням і дублюванням напрямків діяльності органів виконавчої влади загальної та спеціальної компетенції щодо забезпечення інформаційної безпеки тощо.

3. Зважаючи на це, визначено шляхи вдосконалення організаційноправових механізмів державної політики у сфері інформаційної безпеки України, які передбачають адаптацію в Україні світового досвіду

(зокрема, США) щодо створення єдиної державної інформаційно-комунікаційної інфраструктури. Вона, з одного боку, передбачає формування стійкої організаційно-інформаційної мережі та системи, а з другого – покликана забезпечити системне «виробництво – споживання – захист» інформаційних і комунікаційних засобів, продуктів і послуг. При цьому уточнено модель міжсекторної взаємодії щодо забезпечення інформаційної безпеки.

4. На підставі аналізу стану організаційно-функціонального та правового забезпечення державної політики у сфері інформаційної безпеки обґрунтовано новітні функціонали системи державного управління, покликані забезпечити комплексне дотримання основоположних державноуправлінських принципів

Їх облік дозволив нам запропонувати шляхи вдосконалення основної та допоміжно-функціональної організаційної структури Міністерства інформаційної політики України. Це можливо шляхом формування його представництв на регіональному рівні, як інститутів з узгодженим розподілом повноважень і сфер відповідальності, а також створення при них регіональних громадських рад.

Проблема інформаційної безпеки характеризується зростаючою роллю інформації в суспільному житті. Сучасне суспільство все більше набуває рис інформаційного суспільства. Інформаційна безпека-одна з проблем, з якою зіткнулося суспільство в процесі масового використання автоматизованих засобів її обробки. Для досягнення поставленої мети було проведено дослідження теоретичних аспектів даної проблеми в контексті забезпечення інформаційної безпеки, загальної теорії та теорії державної безпеки. Важливо також враховувати точки зору провідних вчених.

Основними суб'єктами забезпечення інформаційної безпеки країни є інститути держави і громадянського суспільства. Однак вони самі відчувають аналогічну потребу, тобто вони також є об'єктами інформаційної безпеки. А Інтернет стає найбільш значущим і сучасним інструментом впливу на об'єкти

інформаційної безпеки. Сучасне розуміння сутності Інтернету повинно включати в себе всю сукупність мережевих відносин, політичних інститутів, технологій і технічних засобів, пов'язаних один з одним по комп'ютерно-опосередкованих лініях, а також характеризуватися єдиним часом і простором. Крім того, Інтернет не тільки охоплює все поле політичних комунікацій в сучасному суспільстві, а й модифікує їх, встановлюючи нові принципи

Вступ України до європейської спільноти, тобто до інформаційного суспільства, викликає велику потребу у формуванні на науковому рівні теоретичних засад концепції правового регулювання інформаційних відносин. Сьогодні можна відзначити, що сукупність нормативних правових актів у цій сфері в Україні досягла такої критичної маси за кількістю, що дозволяє і необхідно виділити їх в окремий правовий інститут.

Інформаційне законодавство є основою інформаційного права, яке зазвичай можна розглядати в декількох аспектах: як галузь суспільних відносин, відображених у правових нормах, як наукову дисципліну і навчальну дисципліну.

Інформаційна безпека особистості, суспільства і держави може бути ефективно забезпечена тільки системою заходів, що носять цілеспрямований і комплексний характер. Особливе значення для формування та реалізації політики інформаційної безпеки має грамотне використання політичних інструментів.

Практика вимагає розробки впливових механізмів захисту суспільних інформаційних відносин. Невизначеність у цьому питанні відображена в законах України "Про інформацію" та "Про захист інформації в автоматизованих системах" та інших, які визначають диспозицію правопорушення, а не визначають відповідальність за них в адміністративному та кримінально-правовому аспектах.

В інформаційному праві особливу увагу слід приділяти виявленню та розслідуванню недоліків як внутрішніх, так і зовнішніх правовідносин, їх регулюванню, щоб уникнути помилок у законотворчості та правозастосуванні в

Україні. Метою дослідження є запобігання негативним наслідкам для інформаційного суспільства, запобігання поширенню правопорушень, вчинених з використанням сучасних інформаційних технологій.

Правотворча діяльність повинна ґрунтуватися на наступних принципах наукового забезпечення: системний і комплексний підходи до вирішення проблем правотворчості; ретельне фундаментальне і прикладне теоретичне обґрунтування інновацій (понять, категорій і т.д.); залучення широкого кола вітчизняних фахівців до розробки проектів законодавчих і підзаконних актів. Такі фахівці повинні володіти всебічними знаннями: в галузі права та інформатики, теорії та практики. Вони також повинні знати не тільки досвід зарубіжних країн, а й мати власне оригінальне бачення вирішення проблем, засноване на специфіці реалій нашої країни.

Формування системи інформаційного законодавства поставило проблему її гармонізації на міждержавному рівні з урахуванням міжнародного права (його провідні компоненти - публічне і приватне право). Сьогодні можна визначити, що в міжнародному праві активно формується новий інститут-Міжнародне інформаційне право світової інформаційної цивілізації. У багатьох частинах світу міжнародні стандарти правових норм формуються на рівні типових законів, багатосторонніх конвенцій, угод і т. д.

У російській інформатиці запропоновано новий підхід до правового регулювання суспільних відносин. Виходячи з положень правової інформатики, слід зазначити, що правотворчість має ґрунтуватися на методології системного та комплексного підходів.

Міжнародне інформаційне законодавство має піти шляхом систематизації через кодифікацію-створення системоутворюючого кодексу. Цей кодекс має розвивати Положення про інформаційні відносини, визначені Конституцією України, у тому числі про інформаційну безпеку особистості, суспільства, нації та

держави. Вона повинна поєднувати, удосконалювати і розвивати норми і принципи суспільних відносин, визначені законодавством України; враховувати нормативні акти (угоди, Конвенції) міжнародного права, ратифіковані Україною; узаконити позитивні звичаї в галузі інформаційних відносин і норми суспільної моралі, загальнолюдські цінності, визначені організацією Об'єднаних Націй в її статуті, Декларації прав людини, рішеннях Європейського Союзу та інших загальноприйнятих міждержавних нормативних актах, які сьогодні є стандартами, за якими визначається цивілізація не тільки окремої країни, а й світової спільноти в цілому.

У процесі забезпечення інформаційної безпеки важливо розуміти природу, характер, сутність і зміст загроз і небезпек, а також вміти своєчасно виявляти джерело загрози.

Всі дії, пов'язані із забезпеченням інформаційної безпеки, повинні включати:

- аналіз, оцінка і прогноз загроз і небезпек, ступінь національної уразливості;

- планування запобігання атак, зміцнення потенційних зв'язків, вирівнювання ресурсів інформаційної безпеки;

- вибір засобів протидії, нейтралізації, запобігання нападу, мінімізації збитку від нападу;

- дії щодо забезпечення інформаційної безпеки;

- управління наслідками кібератак та інформаційних воєн.

Аналіз стану інформаційної безпеки показує необхідність вдосконалення системи адміністративно-правового регулювання інформаційної безпеки. Існує необхідність розробки нових засобів, методів і способів забезпечення інформаційної безпеки державного управління, моніторингу інформаційного середовища, наявності загроз і небезпек.

Підвищення інформаційної безпеки вимагає цілеспрямованого вивчення зарубіжного досвіду організації та проведення інформаційних операцій, методів і засобів проведення кібератак, а також моделювання інформаційних атак.

Проведений аналіз дозволяє стверджувати, що система інформаційної безпеки повинна бути Міжвідомчою та ієрархічно організованою. його структура і організація повинні відповідати структурі державного управління з чіткою координацією дій окремих сегментів.

Організація ефективної системи інформаційної безпеки передбачає централізоване управління з конкретними відомчими та адміністративними функціями, що забезпечують моніторинг і контроль за всіма компонентами національного інформаційного простору. Система інформаційної безпеки повинна мати здатність підтримувати важливі параметри свого функціонування, тобто підтримувати стан гомеостазу, у всіх ситуаціях скоординованої багатосторонньої та багатовимірної інформаційної операції.

В цілому система інформаційної безпеки може бути представлена наступними компонентами::

- концептуальні положення державної політики національної безпеки в інформаційній сфері;

- цілі і завдання як відображення об'єктивних потреб особистості, суспільства і держави в реалізації їх інтересів;

- загрози і небезпеки, уразливості і критична інфраструктура, що вимагає максимального захисту;

- ресурси, сили та засоби забезпечення інформаційної безпеки, які створюються відповідно до законодавства України;

- суб'єкти, що забезпечують інформаційну безпеку на державному, регіональному та місцевому рівнях;

- дотримання вимог інформаційної безпеки громадянами та суб'єктами України;

- стан інформаційних інфраструктур України та міжнародної спільноти;

- забезпечення технічної, технологічної та інформаційної незалежності України в галузі інформаційних телекомунікацій.

Так само хотілося б підкреслити, що абсолютну надійність і безпеку в комп'ютерних мережах не зможуть гарантувати ніякі апаратні, програмні та будь-які інші рішення. У той же час звести ризик втрат можливе лише при комплексному підході до питань безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення. Київ: Ред. журн. «Право України»; Харків: Право, 2013. - 128 с.

2. Арістова І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики: монографія. Харків: Нац. ун-т внутр. справ, 2006. 354 с.

3. Арістова І.В.Державна інформаційна політика: організаційно-правові аспекти. Харків: УВС, 2000. 368с.

4. Безпека комп'ютерних систем. Злочинність у сфері комп'ютерної інформації і її попередження. / ред. О.П. Снігірьов. Запоріжжя: Павел, 1998. 315 с.

5. Богуш В. Інформаційна безпека держави / Володимир Богуш, Олександр Юдін; Гол. ред. Ю. О. Шпак. Київ: "МК-Прес", 2005.432 с.

6. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення ОВС України. *Форум права.* 2009. № 1. С. 50-55

7. Братель О. Поняття та зміст доктрини інформаційної безпеки// Право України.- К., 2006.- 5.- С.36-41.

8. Бутузов В., Гуцалюк М., Цимбалюк В. Протидія злочинності у сфері високих технологій. Міліція України. 2002. № 9. С 20-21.

9. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій: Посібник / Авт. кол.; За ред. Я.Ю. Кондратьева. Ки: НАВСУ: МНДЦ, 2000. - 64 с.

10. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ, 2000. С 50-52.

11. Голубев В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна

безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Монографія / За заг. ред. докт. юрид. наук Р.А. Калюжного. Запоріжжя: Просвіта, 2001. 252 с.

12. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т.Шевченка.* 1999. Вип. 14: Міжнародні відносини. С. 46-48

13. Гуцалюк М. Інформаційна безпека України: нові загрози // Бизнес и безопасность. 2003. № 5. С. 2-3

14. Дзьобань О.П. Національна безпека України: концептуальні засади та світоглядний сенс: Монографія. Харків: Майдан, 2007. 284 с

15. Закон України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" № 1105-XIV від 23.09.1999.

16. Закон України "Про інформацію" від 2 жовтня 1992 р. // Відомості Верховної Ради України. 1992. № 48. Ст. 650.

17. Закон України "Про Концепцію Національної програми інформатизації" від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. 1998. № 27-28. Ст. 182.

18. Закон України "Про охорону праці" № 2695-XII від 14.10.1992.

19. Закон України „Про основи національної безпеки України" від 19 червня 2003 р. № 964 - IV // Офіційний вісник України. № 29. с. 38. Ст. 1433.

20. Закон України «Про захист інформації в автоматизованих системах» №2594 від 31 травня 2005 р.// Офіційний вісник України. К., 2005.24. С.17-20.

21. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»: від 31.05.2005 р., № 80/2005-ВР // Відомості Верховної Ради України - 2005. - № 13. - Ст. 288

22. Закон України «Про основні засади розвитку інформаційного

суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V //Відомості Верховної Ради України (ВВР), 2007, N 12, ст.102

23. Закон України «Про телекомунікації» від 18.11.2003 № 1280-IV//Відомості Верховної Ради України (ВВР), 2004, N 12, ст.155

24. Зеркалов Д.В. Охорона праці в галузі: Загальні вимоги. Навчальний посібник. К.: «Основа». 2011. 551 с.

25. Зеркалов Д.В., Полукаров Ю. О. Організація та управління безпекою життєдіяльності. Навч. посіб. К.: Основа, 2011. 236 с. http://www.zerkalov.org/files/OtaUBG.doc

26. Інформатизація, право, управління (організаційно-правові питання): Монографія / Р.А. Калюжний, О.Д. Крупчан, В.Д. Гавловський, М.В. Гуцалюк, М.Я. Швець, В.С. Цимбалюк; За заг. ред.: М.Я. Швеця, О.Д. Крупчана. - К.: НДЦ правової інформатики АПрНУ, 2002. - 191 с.

27. Інформаційна безпека людини як споживача телекомунікаційних послуг// Арістова І. В., Сулацький Д. В. К.: Ред. журн. «Право України»; Х.: Право, 2013. 184 с.

28. Інформаційне насильство та безпека: світоглядно-правові аспекти// Дзьобань О.П., Пилипчук В.Г. / За заг. ред. проф. В.Г. Пилипчука. Харків: Майдан, 2011. 244 с.

29. Інформаційне право (основи теорії і практики) // В.С. Цимбалюк. Київ: Освіта України, 2010. 388 с.

30. Інформаційне право та інформаційна безпека // Сучасний стан, поняття та визначення змістовної частини, інкорпорація нормативних актів з правових питань у сфері інформації та її захисту: Наук, видання / В.Д. Гавловський, О.І. Коваленко, В.К. Гіжевський, В.С. Цимбалюк та ін.; За заг. ред.: Р. Калюжного, В. Філонова. К.; Донецьк: Донецький ін-т внутр. справ МВС України: Ін-т екон. та права "КРОК", 2001. 230 с

31. Інформаційне право та правова інформатика в сфері захисту персональних даних// В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець. Київ: ТОВ “ПанТот”, 2005. 451 с.

32. Інформаційне право України: підручник// Марущак А.І. Київ: Дакор, 2011. - 456 с.

33. Інформаційне право України: теорія і практика // І.Б. Жиляєв. Київ: Парламентське видавництво, 2009. 104 с.

34. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства // В.С. Цимбалюк. Київ: Освіта України, 2011. 426 с.

35. Інформаційне право: навчальний посібник// В.А. Буржинський, В.Я. Горбачевський, І.В. Мартиненко, Б.Л. Раціборинський,В.М. Смаглюк, В.Г. Хахановський, М.Я. Швець; за аг. ред. В.В. Дурдинця. К.:ДІІ “Друкарня МВС України”, 2009 р. 218 с.

36. Інформаційне суспільство. Дефініції... / В.М. Брижко, А.А. Орехов, В.С. Цимбалюк, О.Н. Гальченко, А.М. Чорнобров; За ред.: Р.А. Калюжного, М.Я. Швеця. К.: Інтеграл, 2002. 220 с

37. Кодекс про адміністративне судочинство: Закон України // Відомості Верховної Ради (ВВР). 2005. № 35-37. Ст. 446

38. Комп'ютерна злочинність: Навч. посіб. / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк, В.Д. Гавловський та ін. К.: Атіка, 2002. 240 с

39. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти// П.Д. Біленчук, М.В. Гуцалюк, О.В. Кравчук, М.В. Козир; за заг. ред. П.Д. Біленчука. К.: Наука і життя, 2008. 291 с.

40. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. 1996. №30 Ст. 141.

41. Концепция информационной безопасности РФ. Утверждена Указом

Президента РФ от 10 января 2000 г. № 24 // Российская газета. 2000. № 24.

42. Концепція (основи державної політики) інформаційної безпеки України. Проект УЦЕПД // Національна безпека і оборона. 2001. № 1. с. 50 - 60.

43. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: дис. … д-ра юрид. наук: 12.00.07 / Борис Анатолійович Кормич. - О., 2004. 427 с.

44. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. К.: Кондор, 2005. 382 с.

45. Кормич Б.А. Деякі проблеми інформаційної безпеки в Україні // Держава і право: Зб. наук. праць. Юридичні і політичні науки. К.: Ін-т держави і права ім. В.М. Корецького НАН України, 2001. Вип. 14. С. 180 - 185.

46. Кормич Б.А. Інформаційне право Підручник. Рекомендовано МОН України для вищих навчальних закладів. Харків: Бурун і К, 2011. 334 с.

47. Кормич Б.А. Інформація як категорія інформаційного права. *Актуальні проблеми держави і права: Зб. наук. праць*. Одеса: Юридична література, 2002.Вип. 16 С. 367 - 374.

48. Кормич Б.А. Концептуально-методологічні засади аналізу правового регулювання інформаційної безпеки // Актуальні проблеми політики: Зб. наук. праць. Одеса: Юридична література, 2003. Вип. 17. С. 89 - 94.

49. Кормич Б.А. Правові методи попередження та ліквідації загроз інформаційній безпеці людини. *Митна справа. Науково - аналітичний журнал з питань митної справи та зовнішньоекономічної діяльності*. 2002. № 5. С. 75 - 83.

50. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти. Монографія. Київ: ТОВ «ДКС», 2012. 342 с.

51. Левицька М. Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України: дис. … канд. юрид. наук: 12.00.01 /

Марина Борисівна Левицька. К., 2002. 206 с.

52. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: [навч. посібник] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К.: КНТ, 2006. 280 с.

53. Ліпкан ВА. Теоретичні основи та елементи національної безпеки України: Монографія. Київ: Текст, 2003. 600 с.

54. Макаренко В. Правове регулювання захисту конфіденційної інформації, що є власністю держави: становлення, розвиток, проблемні питання / В. Макаренко. Право України. 2006. № 1. С. 132-135.

55. Максименко Ю. Є. Сучасні проблеми криміналізації інформаційної сфери. Актуальні проблеми політики: Зб. наук. праць. / Голов. ред. С. В. Ківалов; відп. за вип. Л. І. Кормич. Одеса: ПП "Фенікс". 2005.Вип. 26.С. 294-299.

56. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Ірина Маракова, Анатолій Рибак, Юрій Ямпольский,; Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій .Одеса, 2001. 164 с.

57. Олійник О. Захист інформації в умовах інформаційного суспільства / О. Олійник // Право України. 2005. № 10. С. 100-103.

58. Основи інформаційного права України. В. Цимбалюк, В. Брижко, В. Гавловський; за ред. М. Швеця, Р. Калюжного, П. Мельника. - [2-е вид., допов.]. - К.: "Знання", 2009 р. 414 с.

59. Основи інформаційного права України// В. Цимбалюк, В. Гавловський, В. Гриценко; за ред. М. Швеця, Р. Калюжного та П. Мельника. Київ: "Знання", 2004. 274 с.

60. Правове забезпечення інформаційної діяльності в Україні/ Володимир Горобцов, Андрій Колодюк, Борис Кормич та ін.; Ред. І. С. Чиж; Ін-т держави і права ім. В.М.Корецького, Нац. Академія Наук України, Держ. комітет

телебачення і радіомовлення України. К.: Юридична думка , 2006. 384 с.

61. Правове забезпечення соціальної політики України в умовах розвитку інформаційного суспільства // Савінова Н. А., Ярошенко А. О., Литва Л. А. - К.: Вид-во НПУ імені М. П. Драгоманова, 2012. 270 с.

62. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посіб. / В.О. Голубєв, В.Д. Павловський, В.С. Цимбалюк; За заг. ред. Р.А. Калюжного. Запоріжжя: ГУ "ЗІДМУ", 2002. 292 с

63. Проблеми інформаційного права та правової інформатики// В. Брижко, В. Цимбалюк, В. Гавловський, Ю. Базанов; за ред. М.Я. Швеця і Р.А. Калюжного. Київ: НДЦПІ АПрН України, 2004 р. 263 с.

64. Сировой О. В. Організаційно-правові засади управління інформаційними ресурсами органів внутрішніх справ України: Автореф. дис. … канд. юрид. наук: 12.00.07 / Харк. нац. ун-т внутр. справ. - Х., 2006. - 20 с

65. Соснін О. Національні інформаційні ресурси у сучасних умовах: проблемні питання вітчизняного законодавства. Право України. 2003. № 10. С. 124-128..

66. Стеценко С. Г. Адміністративне право України: [Навчальний посібник]. К.: Атака, 2008. 624 с.

67. Теорія держави та права: [підручник] / С. Л. Лисенков, А. М. Колодій, О. Д. Тихомиров, В. С. Ковальський; За заг. ред. С. Л. Лисенкова, В. В. Копейчикова. Київ: Юрінком Інтер, 2005. 448 с.

68. Цимбалюк В.С. Інформаційне право (основи теорії і практики). Монографія. Київ:"Освіта України", 2010 388с.

69. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства: монографі. Київ: "Освіта України", 2011. 426с.

ДОДАТКИ

Додаток А

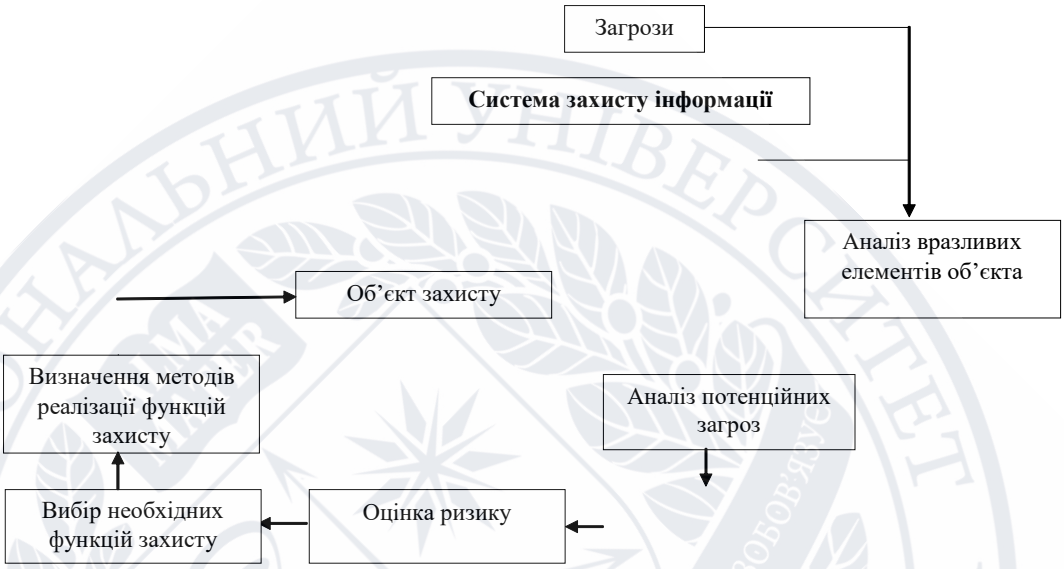

Рис. 1. Система захисту об'єкта