МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
КИЇВСЬКИЙ ІНСТИТУТ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ
ФАКУЛЬТЕТ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ
КАФЕДРА ДЕРЖАВНОЇ БЕЗПЕКИ

«МАГІСТЕРСЬКА РОБОТА ЗА ФАХОМ»

Тема: «Інформаційна безпека України в умовах воєнного стану»

здобувача вищої освіти
другого (магістерського) рівня вищої освіти освітньо-професійної програми 251 «Державна безпека»
Спеціалізація – Організація забезпечення державної безпеки підрозділами Національної гвардії України
Павлушкіна Павла Олександровича
Науковий керівник:
Полковник Островський Сергій Олександрович
кандидат юридичник наук, доцент

Магістерська робота захищена
з оцінкою_____
«___»_____ 20__ р.

Київ – 2025

ЗМІСТ

ВСТУП

Актуальність теми. Повномасштабне вторгнення на територію України відбулось наприкінці зими 2022 року, є однією з найтрагічніших подій історії. Вона забрала життя тисяч людей, призвела до масового руйнування інфраструктури та завдала непоправного болю українському народу.

В умовах війни, як і в будь-якій іншій надзвичайній ситуації, зростає загроза інформаційній безпеці України, через загрози кібератак, інформаційної агресії та пропоганди зі сторони рф.

Актуальність цієї роботи обумовлена необхідністю ретельного вивчення та аналізу інформаційної агресії та кібератак в інформаційному просторі України у контексті збройної агресії сусідської країни, що є важливим внеском у розуміння глобальних проблем захисту інформації та запобігання подібним порушенням інформаційної безпеки в майбутньому.

Мета наукової роботи є аналіз стану інформаційної безпеки в Україні в умовах воєнного часу, вивчення основних загроз та викликів, а також розгляд заходів, що вживаються для забезпечення захисту національної інформаційної інфраструктури. У роботі буде розглянуто роль державних органів, приватних компаній та громадських організацій у забезпеченні інформаційної безпеки, а також важливість міжнародного співробітництва в боротьбі з кіберзагрозами.

Завдання:

1. окреслити поняття: “інформаційна безпека”, “пропаганда”, “кібербезпека”.

2. проаналізувати рівень державного захисту інституту інформаційного простору.

3. проаналізувати процес керування ризиками та небезпеками, що гарантує інформаційну незалежність України.

4. розглянути стан охорони національних інтересів України в інформаційному просторі.

5. розглянути стан охорони законодавчих норм, що регулюють інформаційні процеси в державі.

6. розглянути стан методів та засобів ведення інформаційної боротьби.

7. розглянути стан захисту законодавчо встановлених правил, що регулюють інформаційні процеси в країні.

8. розглянути ризики інформаційній безпеці.

9. розглянути вплив воєнного стану на інформаційну безпеку в Україні.

Об'єкт дослідження: Об'єктом дослідження є інформаційна безпека України в умовах воєнного часу, а саме система забезпечення захисту інформації, управління інформаційними потоками та реагування на інформаційні загрози, які виникають в умовах війни, зокрема в контексті гібридної війни та збройного конфлікту з російською федерацією.

Предметом дослідження є механізми та заходи інформаційної безпеки України, спрямовані на захист національних інтересів та забезпечення стабільності держави в умовах воєнного часу. Це включає в себе вивчення інформаційних загроз, засобів протидії інформаційним атакам, а також аналіз законодавчої, організаційної та технічної бази для забезпечення безпеки в інформаційному просторі.

Наукова робота має практичне та теоретичне значення. Теоретичному вона сприятиме кращому розумінню інформаційної безпеки держави, а практично – допоможе у покращенні заходів щодо запобігання та захисту інформаційного простору України.

Опис трудових функцій:

ҐЗ.З2. Призначення, тактико-технічні характеристики та бойові можливості штатних засобів зв’язку підрозділу;

правила ведення радіообміну, телефонних переговорів, передачі даних по відкритих каналах зв’язку;

відомості, які заборонено передавати засобами радіозв’язку.

ҐЗ.УЗ. Користуватися інформаційно-телекомунікаційними сервісами розгорнутими в підрозділі.

Ґ3.У6. Безпечно користуватися сервісами мережі Інтернет.

Ґ2.У5. Оцінювати обстановку та передавати дані через програмні комплекси.

Ґ3.К1. Застосовувати різні способи комунікації під час організації та забезпечення зв'язку в підрозділі.

Наукова новизна одержаних результатів у межах даного дослідження здійснено комплексний аналіз інформаційної безпеки України в умовах воєнного стану, що дозволило визначити нові загрози та виклики, спричинені повномасштабною військовою агресією.

Розширено підходи до оцінки впливу інформаційної війни та кібератак на національну безпеку, уточнено роль державних, приватних та міжнародних структур у протидії інформаційним загрозам.

Вперше систематизовано сучасні механізми інформаційного захисту в умовах збройного конфлікту, що сприяє розробці ефективних стратегій кібербезпеки та інформаційної оборони держави.

Теоретичною основою даного дослідження. Теоретичною основою даного дослідження є комплексний аналіз сучасних теорій і концепцій, пов'язаних із інформаційною безпекою, кібербезпекою та управлінням в умовах воєнного стану. Робота враховує ключові аспекти кібербезпеки, теорію конфліктів, а також взаємодію інформаційних технологій та воєнного виміру. Широкий обсяг теоретичних джерел, використаних у роботі, дозволяє підтримати обґрунтування та аналіз результатів наукового дослідження.

Методи дослідження, що використовувались під час написання наукової роботи:

1) Аналіз — для вивчення наявних нормативних актів, політик та заходів щодо забезпечення інформаційної безпеки в Україні в умовах воєнного часу.

2) Порівняльний метод — для порівняння підходів та стратегій забезпечення інформаційної безпеки в Україні та інших країнах, що мають подібний досвід в умовах війни або гібридних конфліктів.

3) Метод системного підходу — для вивчення інформаційної безпеки як цілісної системи, що включає різні елементи: технологічні, організаційні, правові, соціальні.

4) Метод експертних оцінок — для визначення ефективності різних методів захисту інформації та оцінки рівня інформаційної загрози в умовах війни.

5) Історичний метод — для вивчення розвитку інформаційної безпеки в Україні, особливо в контексті військових дій та гібридної війни.

Ці методи дозволяють всебічно дослідити проблеми та виклики інформаційної безпеки в Україні в умовах воєнного часу та розробити рекомендації для поліпшення захисту держави від інформаційних загроз.

Нормативною основою роботи. Нормативною основою роботи є вивчення та аналіз діючого законодавства України з питань інформаційної безпеки, кібербезпеки та регулювання умов воєнного стану. Враховуються відповідні норми Кримінального кодексу, Закону України "Про інформацію", Закону "Про кібербезпеку", а також інших відповідних правових актів. Результати дослідження розглядаються в контексті чинної нормативної бази для розробки рекомендацій та стратегій щодо підвищення рівня інформаційної безпеки в умовах воєнного стану.

Структура наукової роботи. Наукова робота складається з вступу, трьох розділів, що містить в собі 9 підрозділів, висновків та списку використаних джерел. Список використаних джерел містить в собі 60 найменувань.

Апробація результатів роботи. Результати роботи були повідомлені, обговорені та схвалені на наступних семінарах, конференціях, круглих столах:

1. Островський С.О., Павлушкін П.О. Проблемні аспекти забезпечення інформаційної безпеки держави під час дії воєнного стану. *Сучасні наукові тенденції в роботах молодих вчених: матеріали II наук.-прак. конф. (Київ, 24*

квіт. 2024 р.), Київ; Київський інститут Національної гвардії України, 2024. С.127-129.

2. Мудра С. В., Павлушкін П.О. Засоби масової інформації в контексті інформаційної безпеки. *Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії*: *матеріали* І *всеукр. наук.-прак. конф. (Київ, 26 квіт. 2024 р.),* Київ; Київський інститут Національної гвардії України, 2024. С.109-112.

3. Островський С.О., Павлушкін П.О. Дезінформація як зброя гібридної війни. *Актуальні проблеми забезпечення державної безпеки: матеріали ІІ всеукр. наук.-прак. конф. (Київ, 25 жовт. 2024 р.),* Київ; Київський інститут Національної гвардії України, 2024. С.417-421.

4. Толстоносов Д. Ю., Павлушкін П.О. Важливість логістичного забезпечення для стійкості національної кібербезпеки. *Актуальні проблеми теорії та практики службово-бойової діяльності складовий сектору безпеки та оборони в сучасних умовах*: *матеріали ІІ всеукр. наук.-прак. конф. (Київ, 24 трав. 2024 р.),* Київ; Київський інститут Національної гвардії України, 2024. С.261-263.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

1.1 Природа понять: інформаційна безпека, кібербезпека, воєнний стан

У сучасних умовах інформація впливає на формування якісних архетипів національного керування та реалізації цих архетипів. При цивілізованому підході, ця ідея є прикладом дій та реалізації уряду. Кожному гарантується право на інформацію на конституційному рівні. Оскільки інформація має великі можливості як соціально-правове явище, маніпулювання інформаційними потоками з метою дестабілізації певних сфер суспільних відносин є закономірністю.

Пошук засобів впливу на формування та підтримку належного рівня інформаційної безпеки в Україні є важливим через:

а) війни росії проти нашої держави;

б) цифровізацією правовідносин та переходом інформаційних матеріалів до цифрової площини;

в) Глобалізація суспільних відносин з неоднозначністю, яка супроводжує національні кордони з точки зору розподілу, споживання та розподілу інформації.

Поняття "національна безпека" відображає рівень врегулювання суспільних відносин в країні та підкреслює важливість забезпечення національної ідентичності діє через гарантування захисту національного суверенітету, національної інтеграції, демократичного конституційного порядку.

Посилаючись на актуальну нормативно-правову базу, яка займається аспектами реалізації обороздатності країни, розрізняються основні принципи її структурування через класифікацію національної безпеки за галузево-

видовою ознакою та залученими суб'єктами. Це обумовлено тим, що безпека держави є складним і множинним соціально-правовим явищем.

За галузево-видовою ознакою безпека держави включає: військову, суспільну, державну, кібернетичну, зовнішню політичну, публічну, екологічну безпеку, фінансову та інформаційну безпеку.

За примітивними рисами безпеки країни розуміються дії урядів, збройних сил, правоохоронних та розвідувальних органів, ключових державних органів з правоохоронними повноваженнями, сил цивільної оборони, а також окремих осіб та неурядових організацій, які добровільно взяли на себе зобов'язання щодо зміцнення безпеки України.

Тому галузь державної безпеки можна визначити як сукупність правовідносин, у яких визначена роль уповноваженої особи забезпечити загальну безпеку країни, з врахуванням різних напрямів.

Приділимо увагу тому, що згідно з українським законодавством, концепції «військової безпеки», «державної безпеки» та «національної безпеки» є взаємопов'язаними. Перша стосується захисту від військових загроз, що визначаються державою; друга - від реальних або потенційних загроз невоєнного характеру; третя - забезпечення загальної захищеності, зокрема в умовах різної природи загроз [1, с. 60-61].

Зробимо відомим, що:

а) першочерговим є об'єкт, який потребує захисту;

б) національна безпека, в такому випадку, охоплює державну безпеку та безпеку воєнного характеру;

в) тісний зв’язок між національною безпекою та військовими може бути досягнутий лише шляхом вираження права збройних конфліктів. Тому вбачається за необхідне внести зміни до Закону про національну безпеку України та уточнити положення закону.

На основі того, що об'єкт, який потребує захисту, є першорядно важливим; національна безпека, яка включає державну та військову безпеку, здійснюється лише через посилання на правову природу загрози. У внесенні

змін до Закону України "Про національну безпеку" доцільним буде викласти його зміст таким чином:

"Національна безпека України – забезпечення державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз незалежно від їх характеру". Тим часом, визначення "державна безпека" слід виключити, оскільки національна безпека є його формальним відображенням.

Сучасний стан інформаційного законодавства України вимагає невідкладних заходів для його оптимізації, оскільки його недоліки стають все більш помітними. Проте серед науковців, які займаються цим питанням, не спостерігається консенсусу щодо стратегій ефективного оновлення законодавства. Така розбіжність думок може бути викликана складністю, динамічністю та широким охопленням сучасних інформаційних процесів у контексті формування національної правової системи.

Зокрема, В. Горбулін та М. Биченко висловили думку, в разі якщо найкритичнішою ситуацією у сфері інформаційного захисту є відсутність в суспільстві та науковому співтоваристві уніфікованого розуміння концепції інформаційної безпеки із юридичної перспективи. Це вказує на необхідність більш глибокого аналізу та розвитку теоретичних підходів в цій галузі.

Застосування системного підходу у сфері формування права та нормотворення є нагальною потребою, обумовленою відсутністю адекватної систематизації діючого інформаційного законодавства.

Відсутність методологічних засад для створення норм інформаційного права призводить до об'єктивних та суб'єктивних труднощів у процесі становлення системи нормативно-правового регулювання інформаційної безпеки. Належне відображення сучасних умов в усвідомленні нормотворців є критичним для вдосконалення інформаційного законодавства, необхідно враховувати різноманітні аспекти інформаційної безпеки, включаючи психологічні, технічні та правові складові.

Як спостерігається, концепція інформаційної безпеки не може бути класифікована як першорядна і повинна бути аналізована в контексті соціальної безпеки і використання її методологічних ресурсів. Визначення терміну "безпека" як основної категорії має критичне значення для глибинного дослідження інформаційної безпеки.

Враховуючи те, що безпека є явищем соціальним, належна увага має бути приділена філософсько-соціологічній інтерпретації, яка має служити фундаментом для системного підходу в осмисленні безпеки. Це підход, у свою чергу, сприятиме уникненню використання неоднозначних і суперечливих термінологій, таких як "захищеність", "інтереси", "потреби", і "загрози" у наукових визначеннях, демонструючи при цьому синергетичний аспект явища безпеки.

Основу представленого підходу розробив Г. Іващенко, який критикує загальноприйняте визначення безпеки як стану захищеності відповідних критичних інтересів суспільства від потенційних внутрішніх та зовнішніх загроз. Замість цього, він акцентує на необхідності усвідомлення безпеки через діяльнісний підхід, який був розроблений у рамках соціальної філософії та теоретичної соціології [2, с. 34-38].

Водночас, цей підхід не передбачає формальне розуміння безпеки як виду діяльності, ізольоване від її результатів, умов реалізації та здатностей суб’єкта діяти в цих умовах. З цієї перспективи безпека визначається як «сукупність умов існування суб’єкта, які той оволодів, освоїв та створив у процесі самореалізації і які він здатен контролювати».

В контексті синергетичного аспекту слід визначити взаємозалежність між умовами суб’єктивної сторони правовідносин та його здатностями або можливостями їх регулювання та управління. Причини створення можуть функціонувати як каталізатори розвитку здатностей суб’єкта та підвищення його спроможностей, зумовлюючи далі його здатність модифікувати ці умови з метою їх покращення.

Навіть потенційні загрози, які не викликають дестабілізації діяльності суб’єктів, можуть стимулювати процеси саморозвитку. Відповідно, одним із базових завдань держави визначається створення мінімальних умов, які сприятимуть самостійному розвитку особистостей та їхній самореалізації.

В контексті синергетичного аспекту слід визначити взаємозалежність між умовами існування суб’єкта та його здатностями або можливостями їх контролю. Умови існування можуть функціонувати як каталізатори розвитку можливостей суб’єкта та підвищення його спроможностей, зумовлюючи далі його здатність модифікувати ці умови з метою їх покращення.

Навіть потенційні загрози, які не викликають дестабілізації діяльності суб’єктів, можуть стимулювати процеси саморозвитку. Відповідно, одним із базових завдань держави визначається створення мінімальних умов, які сприятимуть самостійному розвитку особистостей та їхній самореалізації.

На сучасному етапі відсутній уніфікований підхід та консенсус серед науковців щодо точного визначення поняття "інформаційна безпека". У специфічній концептуальній рамці інформаційну безпеку в Україні можна розглядати як інтеграцію важливих умов, які забезпечують діяльність суб'єктів інформаційної сфери (особи, суспільства, держави) та їхні суб'єктивні аспекти (правові, політичні, інформаційні, наукові, операційні та дослідницькі) для розуміння та управління цими умовами.

В цьому контексті, інформаційна безпека набуває різного роду характеру. Об'єктивна сторона інформаційної безпеки включає умови, які концептуально мають забезпечувати ефективне функціонування та розвиток суб'єктів, та на рівні загальноприйнятих стандартів безпеки відображають відносний та узагальнений характер цих умов.

Отже, законність формує невід'ємний організаційно-ідеологічний фундамент, який є критично важливим для досягнення стратегічних цілей у таких сферах, як розвиток громадянського суспільства та становлення правової держави.

У контексті інформаційного простору суспільства та держави, законність виступає як каталізатор таких процесів, сприяючи стабільному інформаційному розвитку, ефективній взаємодії між державою та громадянами, а також між самими громадянами, що в кінцевому результаті сприяє зберіганню інформації високого рівня.

Практичне забезпечення принципу легітимності в країні має на меті створення ефективної системи гарантій, ефективність яких визначається реальністю застосування законності. Варто підкреслити, що гарантії законності об'єднують в собі широкий спектр комплексних заходів з значним юридичним та суспільним змістом [3, с. 28-33].

В сучасному інформаційному світі кібербезпека стає все більш важливою для наукових досліджень, які набирають обертів щороку. Останнім часом дослідники активно займаються кібербезпекою та її різними аспектами. Однак проблема усвідомлення цієї проблеми залишається актуальною, враховуючи швидкі темпи розвитку електронної сфери.

Це пояснюється збільшенням можливостей інформаційного впливу на суспільство, що породжує нові загрози громадській безпеці та потребу у вдосконаленні систем безпеки. Також поняття кібербезпеки вимагає переосмислення через стрімкі зміни в інформаційному середовищі та головні тенденції у розвитку світового співтовариства.

Д. О. Беззубов визначає такі характеристики категорії "безпека" як постійність, структурність, системність, альтернативність, визначеність, конкретність досягнень, результативність, статичність, особистісне та колективне спрямування, прогнозованість.

У наукових дослідженнях відсутнє загальноприйняте розуміння поняття "кібербезпека". Існує необхідність уточнення цього поняття для більш глибокого розуміння перспективних змін в галузі кібербезпеки та для надання йому системного характеру, що є вкрай важливим.

За визначенням Кормича Б., кібербезпека — це захист законодавчо встановлених норм, що регулюють інформаційні процеси в державі,

забезпечуючи умови для існування та розвитку людини, суспільства та держави, які затверджені Основним законом.

Автори пропонують таке визначення "кібербезпеки", як стан захищеності особи, держави та суспільства, за якого забезпечується інформаційний розвиток та зовнішні інформаційні впливи не завдають їм значної шкоди.

Деякі вчені розуміють термін «кібернетична безпека» як забезпечення оборони матеріальних об’єктів для нормального їх функціонування навіть у випадку внутрішніх та зовнішніх інформаційних впливів.

Кібербезпека — це сукупність заходів, процесів, технологій та політик, спрямованих на захист інформаційних систем, мереж, програм, даних і цифрових активів від кіберзагроз і атак. Вона охоплює як захист від зовнішніх, так і внутрішніх загроз, сприяючи забезпеченню конфіденційності, цілісності та доступності інформації, а також надійності цифрових інфраструктур і технологій.

Кібербезпека важлива для забезпечення безпеки держави, бізнесу та особистої інформації в умовах все більшої цифровізації суспільства. У сучасному інформаційному суспільстві система забезпечення кібербезпеки України розвивається згідно з актуальною законодавчою базою.

Ця система ґрунтується на органах, силах та засобах забезпечення кібербезпеки, які використовують різноманітні заходи з різних сфер управління для забезпечення стійкого функціонування системи державного управління [4, с. 388].

Відповідно до статті 2 Закону України "Про основи національної безпеки України", правову базу У галузі національної безпеки України основу складають Конституція, закони України, міжнародні угоди, ратифікація яких здійснена Верховною Радою України, а також інші нормативно-правові документи, видані для реалізації законодавства.

Серед таких актів можна виділити такі закони України: "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки",

"Про Концепцію Національної програми інформатизації", "Про Національну програму інформатизації", "Про інформацію", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про доступ до публічної інформації"; Проект закону України "Про Концепцію національної інформаційної політики"; Указ Президента України "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері кібербезпеки України".

Режим воєнного стану є важливою складовою системи національної безпеки в багатьох країнах світу. Згідно із чинним законодавством України, воєнний стан є спеціальним правовим режимом, що цей режим вводиться у разі військової агресії або загрози нападу на Україну, а також при загрозі державній незалежності чи територіальній цілісності.

Цей режим передбачає передачу відповідним державним органам, військовому командуванню, військовим адміністраціям та місцевим органам самоврядування необхідних повноважень для захисту від загроз, запобігання агресії, забезпечення національної безпеки, а також для усунення загроз державній незалежності та територіальній цілісності. Окрім того, це включає тимчасове обмеження конституційних прав і свобод громадян та прав і законних інтересів юридичних осіб, з визначенням терміну таких обмежень.

У багатьох країнах світу режим воєнного стану є важливою складовою частиною системи національної безпеки. Відповідно до чинного законодавства України, воєнний стан є особливим правовим режимом, який вводиться на території країни або в окремих її регіонах у разі збройної агресії чи загрози нападу, що ставить під загрозу державну незалежність та територіальну цілісність України.

Це включає надання необхідних повноважень державним органам, військовому командуванню, військовим адміністраціям та місцевим органам самоврядування для запобігання загрозам, відвертання збройної агресії та забезпечення національної безпеки. Водночас цей режим передбачає

тимчасові обмеження конституційних прав і свобод громадян та юридичних осіб, які зумовлені наявною загрозою, із зазначенням терміну їх дії.

Протягом останніх років в Україні активно обговорювалася необхідність введення режиму воєнного стану. Восени 2018 року, через посилення агресії з боку російської федерації, цей режим був введений в окремих східних та південних регіонах України, а також на внутрішніх водах Азово-Керченської акваторії.

Питання введення "воєнного стану" в Україні має чітку регламентацію як у Конституції, так і в спеціальних законах, зокрема "Про оборону України" та "Про правовий режим воєнного стану". Цей специфічний режим може бути запроваджений по всій території країни та окремих її районів.

Цей режим передбачає надання додаткових повноважень для запобігання загрозам, відвертання збройної агресії та забезпечення національної безпеки. Окрім того, він може тимчасово обмежувати конституційні права і свободи громадян, а також права юридичних осіб на строк, обумовлений загрозою [5, с. 414].

У Конституції чітко зазначено, що під час воєнного стану можуть бути уведені тимчасові обмеження прав і свобод, за винятком тих, які передбачені певними статтями. Іншими словами, режим воєнного стану прямо впливає на процеси всередині країни та винятково стосується внутрішньополітичних процесів.

1.2 Роль і значення інформаційної безпеки для сучасного суспільства

У наш час в інформаційній епохи XXI століття безпека на інформаційному полі набуває все більшого значення, а питання її забезпечення стають все більш актуальними. Швидкий розвиток інформаційних та комп'ютерних технологій у всіх сферах суспільного життя та економіки

підкреслюють потребу у розробці обґрунтованих та ефективних методів для гарантування інформаційної безпеки.

Інформація виступає як основна сила та галузь, яка прагне застосувати передові технології у всіх сферах громадської діяльності. Оскільки інформаційна безпека є ключовим елементом системи безпеки як для окремих країн, так і для суспільства в цілому, це питання привертає увагу як вітчизняних, так і міжнародних науковців, а також широкого кола державних і недержавних наукових установ, дослідницьких та аналітичних центрів.

Термін "інформація" походить від латинського слова "information" і дослівно перекладається як "ознайомлення, пояснення, уявлення, поняття". Часто у наукових працях з питань інформаційної безпеки обмежуються саме цим визначенням, не формуючи конкретного поняття "інформація".

Проте, дослідження наукової літератури показує, що існує безліч визначень сутності інформації, які представляють різні підходи. Важливо проаналізувати інформацію на двох рівнях.

На макрорівні інформація є ключовим фактором могутності держави, оскільки здатність мати доступ до новітніх інформаційних технологій дозволяє ефективно керувати нею. Володіння цією здатністю стає шляхом до посилення економічної сили держави [6, с. 408].

На рівні мікропідприємства, ефективність управління визначається обсягом, достовірністю, цілісністю та якістю обробки інформації, що в свою чергу стимулює Застосування інформаційних технологій в управлінні фінансовими, грошовими та соціально-економічними процесами підприємства є необхідним. Без достатнього обсягу та якості інформації неможливо забезпечити розвиток підприємства на основі передових технологій виробництва та ефективних методів організації праці.

У XXI столітті інформаційна безпека стає важливою складовою національної безпеки держави, внаслідок чого розвиток держави у різних сферах, включаючи економічну та військово-політичну, залежить від забезпеченості правильності та конфіденційності інформації. Тільки держава,

яка забезпечує собі стратегічну і тактичну перевагу, може гнучко регулювати економічні витрати на озброєння та військову техніку, підтримувати передові технології та вести успішну інформаційну боротьбу.

По-перше, В. Гавловський вирішив, що інформація присутня не лише у живих і розумних істот, але й у всіх матеріальних тілах, беручи у розгляд існування інформації в неорганічній природі у потенційній формі. З'являючись у живих організмів, використання інформації для пізнання та управління починається.

По-друге, Р. Калюжний вважав, що інформація має характеристики лише високоорганізованої, тобто живої матерії. Він стверджував, що інформація та інформаційні процеси притаманні лише біологічним та соціальним формам руху матерії, і що живі організми отримують необхідну інформацію через постійну взаємодію з природою та обмін з навколишнім середовищем.

Він акцентував увагу на тому, що інформація відіграє важливу інтегруючу роль, яка допомагає розвивати адаптаційні здібності у живих істот, зокрема у людини. Таким чином, інформація є основою процесів саморегулювання у живій природі.

В третьому рядку, науковці пропонують функціональний підхід до розуміння сутності інформації, згідно з яким інформація є властивістю лише систем, що здатні до самоорганізації, як у живій природі, так і в технічних пристроях. До таких систем відносяться живі істоти та кібернетичні системи, які мають характерні процеси саморегулювання за допомогою передавання, зберігання та оброблення інформації.

У четвертому пункті, вчені пропонують соціалістичний метод вивчення інформації, розглядаючи її як результат життєдіяльності соціальних форм матерії, які існують об'єктивно в процесі та часі, але проявляються лише через пізнання людиною навколишнього світу.

У сучасній науковій парадигмі існують різні теорії, які намагаються пояснити природу інформації, що вказує на її складність та багатогранність.

Важливо зауважити, що в рамках наукових досліджень відсутнє загальноприйняте визначення поняття "інформація", що призвело до різноманітних спроб його визначення.

Це лише маленька частка з різноманітних визначень інформації, які розглядають її різні аспекти. Згідно з думкою вчених, інформація має кілька загальних характеристик: вона не створюється або не знищується, а лише виникає, передається, приймається і може змінювати форму, не змінюючи суті.

Згідно з науковими підходами і законодавством України, інформація - це документовані або оприлюднені дані про події та явища в суспільстві, державі та навколишньому середовищі, в тому числі інформація, призначена для користувачів [7, с. 193-196].

Усі дані, що генеруються та розповсюджуються в Україні, без взаємозалежності від змісту, форми, часу та місця, ці дані складають інформаційні ресурси. Україна має право самостійно формувати ці ресурси на своїй території та використовувати їх, за винятком випадків, передбачених законодавством та міжнародними угодами.

Державні матеріальні відомості становлять основу інформаційного суверенітету України, що гарантується через інформаційну безпеку. Поняття "інформаційна безпека" було вперше використано в кінці 80-х років німецьким вченим Я.М. Жарковим, який акцентував увагу на важливості інформаційного аспекту в міжнародній безпеці. Пізніше в українській та російськомовній пресі почали активно досліджувати проблему інформаційної безпеки як окремого аспекту.

Вивчення походження наукових досліджень та правової практики у сфері забезпечення інформаційної безпеки України дозволив виокремити три основні етапи її розвитку. Як широку наукову категорію, "безпеку" можна визначити як стан системи, коли вона здатна протистояти зовнішнім і внутрішнім загрозам, і її функціонування не становить загрози для самої системи або зовнішнього середовища.

Забезпечення інформаційної безпеки є ключовим аспектом розвитку інформаційного суспільства, що потребує не лише розвитку технологічних можливостей обміну інформацією, але й повідомлення всіма учасниками інформаційних відносин - власниками, користувачами інформації, розробниками технологій, постачальниками послуг і державою - про необхідність захисту матеріальних відомостей та забезпечення безпеки в цій сфері.

Дослідження терміну «інформаційна безпека» є важливою метою наукового дослідження, оскільки воно виражає загальне управління загрозами і ризиками в інформаційній сфері.

В науковій літературі поки що немає однозначного узгодженого розуміння поняття "інформаційна безпека". Для одних це є відображенням стану, для інших – процесом, діяльністю, здатністю, системою гарантій або властивістю чи функцію. Тому виникає необхідність у систематизації різних підходів до визначення даного поняття.

Також важливо визначити головні напрями забезпечення інформаційної безпеки в різних сферах:

- у міжнародній співпраці - згуртування в міжнародній системі гарантування відомчої безпеки та взаємодопомога у запобіганні незаконних махінацій у інформаційній галузі;

- в оборонній галузі:

- удосконалення структури виявлення ризиків та їх похідних першопричин, вчасне повідомлення відповідним авторитетам про стан інформаційних ресурсів та систем у оборонній галузі;

- підходів, методик та інших варіантів оборони, особливих методів та інформаційного впливу;

- організації навчання та гідної підготовки споживачів.

Отже, інформаційна безпека відіграє важливу роль у сталому розвитку держави, і етап гарантування та реалізування інформаційної безпеки повинен розглядатися як одне з основних і найважливіших завдань публічного

керування, яке має включати політичні, економічні, воєнні, культурні та інші аспекти роботи структури керування державним устроєм.

Крім того, важливо розглянути основний зміст, порядок реалізації забезпечення інформаційної безпеки, інструменти, завдання та нормативне регулювання цього процесу, які включають наступне:

1. Забезпечення інформаційної безпеки шляхом впровадження єдиної державної політики національної безпеки в інформаційній сфері.

2. Система забезпечення інформаційної безпеки виступає інструментом реалізації державної політики в цій галузі. Вона складається з організаційного поєднання заходів різного характеру (інформаційного, адміністративного, управлінського, методологічного), спрямованих на забезпечення інформаційної безпеки особистості, суспільства і держави.

3. Завдання цієї системи полягають у наступному:

- моніторинг та прогнозування можливих дестабілізуючих факторів і інформаційних загроз, що можуть вплинути на життєво важливі інтереси особистості, суспільства та держави;

- здійснення оперативних та довгострокових заходів для їх запобігання та усунення;

- створення та підтримка готовності сил і засобів для забезпечення інформаційної безпеки.

- покращення державної політики в галузі розвитку інформаційної сфери, зокрема шляхом створення сприятливих умов для розвитку національної інформаційної інфраструктури та впровадження сучасних технологій у цій сфері.

- гарантування майбутнього аналізу та обробки інформації в країні.

4. Нормативно-правове поле, яке регулює систему забезпечення інформаційної безпеки України, включає Конституцію України, Закон "Про основи національної безпеки України", Закон "Про інформацію", Закон "Про Концепцію Національної програми інформатизації", Указ Президента України "Про заходи щодо розвитку національної складової глобальної інформаційної

мережі Internet та забезпечення широкого доступу до цієї мережі", а також інші законодавчі акти.

5. Функції системи забезпечення інформаційної безпеки України полягають у вдосконаленні нормативно-правової бази для розвитку інформаційних ресурсів, оптимізації державної політики в галузі інформатизації, регулюванні інформаційного співробітництва, а також у контролі за дотриманням встановлених порядків і правил формування та використання інформаційних ресурсів.

Після аналізу різних підходів до визначення "інформаційної безпеки" зрозуміло, що немає варто обирати одну конкретну позицію. Ці підходи дозволяють розглядати це явище в комплексі і системно.

Також слід враховувати, що інформаційна безпека — це не просто стан, а характеристика та ознака інформаційного суспільства, що є результатом діяльності людей, спрямованої на забезпечення безпеки в інформаційній сфері. Інформаційна безпека є процесом, адже вона повинна враховувати перспективу майбутнього [8, с. 56-61].

Також до характеристик інформаційної безпеки слід віднести показники, які мають особливе значення. На кожній керівній гілці влади в Україні визначено різні органи: на стратегічному рівні - Кабінет Міністрів України; на тактичному рівні - центральні органи виконавчої влади; на оперативному рівні - місцеві органи виконавчої влади, зокрема місцеві державні адміністрації, які грають важливу роль.

Ще до важливих аспектів інформаційної безпеки відноситься аналіз показників, які виявляються на кожному рівні державного управління: стратегічному, тактичному та оперативному. У системі забезпечення інформаційної безпеки ключовими елементами є різні рівні, такі як нормативно-правовий, адміністративний, процедурний та програмно-технічний.

Позицію вчених про логіку наукового процесу вважається добре обґрунтованою. Відповідно до цього, ми розглядаємо доцільним аналізувати

різноманітні фактори у частині підвищення рівня розвитку освіченості суспільства та забезпечення інформаційної безпеки.

Психологічний аспект, як частина інтелектуальної сфери, включає ряд характеристик української суспільної свідомості, які мають негативний вплив на інформаційний розвиток суспільства та забезпечення інформаційної безпеки.

1) недооцінка, упередження та байдужість в громадському мисленні;
2) існування нерозвиненої інформаційної культури у загальносуспільній свідомості;
3) неусвідомлення цифрових ризиків;
4) відсутність правосвідомості суспільства;
5) зниження загального освітнього розвитку;
6) розповсюдження юридичного беззаконня;

Динамічний розвиток галузі медіа простору, процес формування, формулювання та реалізації інформаційного права. Цей фактор спричиняє недосконаліть законодавства, що регулює сферу інформаційних відносин у суспільстві, і неефективність його виконання.

Головними передумовами розвитку в інформаційній сфері є:

- швидкий прогрес відомчої галузі;
- різкий прогрес технологій;
- зростаючий рівень складності й всебічності правовідносин у цій галузі;
- новітність медіа-відносин і недостатність досвіду в галузі їх правового регулювання;
- наявність традиційних стандартів у інформаційній сфері, сформованих людством.

Зростання соціальної значущості інформаційних процесів полягає в тому, що визначаються пріоритетні організаційні та практичні заходи, які держава реалізує в інформаційній сфері як основу для подальшого розвитку суспільства. Це підтверджується широким впливом інформаційних процесів, створенням нових можливостей для інформаційного обміну, умовами для

саморозвитку учасників, виникненням нових загроз суспільній безпеці та значним посиленням важливості всіх аспектів інформаційної безпеки.

Економічний фактор забезпечує матеріальну основу для інформаційного розвитку суспільства та держави, а також створює технічні умови для впровадження інформаційно-комунікаційних технологій.

Підсумовуючи сказане, можна відзначити, що стрімкий розвиток наукових досліджень у сфері інформаційної безпеки в 90-х роках минулого століття змінився науковою байдужістю до цієї теми. Наразі відсутні будь-які концептуальні документи з інформаційної безпеки, і аналіз наукових праць свідчить про недостатність досліджень цієї проблеми.

Воно залежить від того, що хоча інформаційна безпека згадується в багатьох нормативних актах і існують десятки документів, присвячених її захисту, вони не мають чіткого визначення поняття і не пояснюють, що саме захищається. Важливо також вивчити підходи до визначення сутності інформаційної безпеки [9].

1.3 Державна політика щодо інформаційної безпеки в умовах воєнного стану

У сучасному політичному процесі громадянське суспільство активно бере участь у формуванні політичних рішень і залученні ЗМІ до обговорення та дискусій. Державна політика піддається зростаючому тиску громадськості як у межах країни, так і за її межами.

Це зумовлено процесом глобалізації інформаційних потоків, які вільно розповсюджуються по всьому світу. Практично завершуються етапи інформатизації суспільно-економічного життя та формування глобального інформаційного простору.

Сучасні технології інформації дали суспільству можливість впливати на діяльність держави та прийняття політичних рішень через громадський

контроль. Це особливо помітно під час подолання кризових ситуацій, коли відбувається мобілізація суспільства та його залучення до процесів.

У разі воєнного конфлікту виникає потреба у розробці ефективної державної інформаційної політики як засобу регулювання взаємодії всіх елементів суспільно-політичної системи, зокрема держави, громадянського суспільства та засобів масової інформації.

У військовій сфері, негативні інформаційні впливи, що зростають під час конфлікту, потребують проведення цілеспрямованої публічно-правової діяльності та регулювання процесів для вирішення оборонних завдань. Успіх цих завдань залежить від рівня політичної культури та свідомості громадян, а також від усвідомлення індивідуумами актуальних потреб і викликів.

Стійкість соціальної системи залежить від скоординованих дій органів влади та громадськості, що забезпечує зв'язок між громадянським суспільством і державою під час військових конфліктів. Протидія негативному впливу на військово-інформаційні ресурси, а також забезпечення ефективного функціонування системи інформаційного забезпечення в військовій та соціально-економічній сферах є ключовими завданнями.

В сучасний період реалізація державної інформаційної політики вимагає її нового теоретичного осмислення. Такий процес тісно пов'язаний з науковою обґрунтованістю і ефективністю впровадження інформаційної політики, а також з її ідеологічним забезпеченням. Існує констатація того, що адміністративно-правові та управлінські науки недостатньо розробили ці питання.

Аналогічна ситуація простежується у сфері інформації: державна інформаційна політика часто розглядається як інструмент, що сприяє корпоративним інтересам держави, тоді як засоби масової інформації, офіційні та неофіційні, вони виконують роль зв'язуючої ланки між державою та громадянським суспільством. Це суперечить об'єктивному факту, що підкреслює незалежність засобів масової інформації (преси) як суб'єкта інформаційної влади [10].

На тлі активного розвитку інформаційних технологій виникає нова інформаційна реальність, що характеризується появою глобальної інформаційної інфраструктури. Цей процес супроводжується зусиллями провідних держав світу зі створення інформаційного суспільства, де особлива увага приділяється аспектам інформаційного панування та контролю над напрямом і змістом інформаційних потоків.

Такі дії викликають появу нових типів протиріч, які більше не можуть бути вирішені за допомогою традиційних методів управління. Паралельно з цим, в контексті глобальної інформатизації стають все більш видимими нові глобальні виклики, особливо у сфері інформаційної безпеки та інформаційних війн.

Не слід зводити всі проблеми виключно до контексту глобальної інформатизації, однак створення єдиного світового інформаційного простору сприяло його перетворенню на арену міжнародних протистоянь. Держави, що мають перевагу у сфері інформаційних ресурсів, часто використовують цю перевагу для інформаційного протиборства з менш могутніми конкурентами.

Активне використання інформаційних технологій у мілітарно-політичній сфері має глибокий вплив на військово-політичну практику, спричиняючи суттєві зміни у військовій стратегії та тактиці досягнення політичних цілей за допомогою сили. Це також призводить до розширення уявлень про військову політику, військово-політичні відносини та інформаційну воєнізацію. Інформаційні війни становлять серйозний виклик для сучасної системи цінностей.

Маніпуляція інформацією шляхом психологічного впливу на опонентів відома як методика ведення військових дій протягом історії. Специфіка інформаційної війни полягає не тільки у використанні сучасних технологічних засобів для реалізації цього впливу, але й у тому, що вона оперує ресурсами, які важко піддаються правовій регуляції, рятуючись неправдивою та спотвореною інформацією як інструментом маніпуляції свідомістю.

В умовах сучасного глобалізованого суспільства спостерігається трансформація ролі держави, державної влади та системи національної оборони в контексті військових конфліктів. Основною метою інформаційної війни є послаблення морального та матеріального потенціалу супротивника або конкурента та підсилення власних сил.

В аналізі сучасних військових конфліктів помітним стає виразний акцент на боротьбі за інформаційну перевагу. Інформаційна перевага традиційно вважається критичною умовою для досягнення перемоги у війні. Однак, під час російсько-українського військового конфлікту, спостерігається посилення акценту на завоюванні та утриманні цієї переваги.

В цьому контексті інформаційно-медійна активність українських державних діячів, зокрема Президента України Володимира Зеленського, може бути розглянута як сучасний вираз такої боротьби [11].

Поряд із традиційним розумінням війни як збройного конфлікту між організованими арміями, використовуючи відповідні людські ресурси та технічні засоби, сучасна воєнна лексика оновилася такими поняттями як "гібридна війна", "інформаційна війна", "кібервійна", "війна компроматів" та іншими, що відображають розширений спектр стратегій та методів ведення війни.

Інтеграція досягнень інформаційної революції з військовою сферою призвела до створення нової сфери діяльності, що відома як військово-інформаційна. У цьому контексті реалізація інтересів різноманітних соціальних груп потребує від керівництва країни, не тільки встановлення чіткої позиції, але й активної участі у встановленні та регулюванні взаємовідносин між цими групами.

Теоретична та методологічна основа формування ідеології інформаційної політики у воєнний період повинна опиратися на сучасні концепції політичної інфо системи.

Така схема вбачається як спектр ідей, установок, цілей, методів та інструментів, який держава використовує через свої органи та представників

для нормативно-правового регулювання стосунків між громадським сектором та інформаційною системою держави, здатною забезпечити владний вплив на суспільні динаміки.

Масові медіа націлені на задоволення інформаційних потреб індивідіумів, які виступають споживачами інформації, забезпечуючи їм доступ до необхідних даних. Це сприяє осмисленій участі особистості у процесах суспільних трансформацій та впливу на соціальну практику. В таких обставинах метою країни є створення нормативно-правової бази, що відповідала б сучасним соціальним вимогам і була високоефективною.

Така база має задавати ключові параметри та регулятивні функції державної інформаційної політики, що структурує взаємодію держави зі засобами масової інформації, а також взаємодію цих засобів із громадянським суспільством. Основним принципом такої політики є забезпечення доступу до інформації, але одночасно важливим є захист державних інтересів від потенційних зловживань приватними засобами друку, зокрема через законодавчі механізми.

З теоретичної перспективи, інформаційна політика розглядається як застосування державних ресурсів та інструментів влади для підбору найбільш ефективних стратегій вирішення актуальних проблем у сфері інформації. Відповідно до статті 6 Закону України "Про інформацію", державна інформаційна політика розглядається як комплекс основних напрямків та способів діяльності держави, що стосуються здобуття, використання, поширення та зберігання інформації [12].

Інформаційна політика задіяна у структуруванні та координації процесів генерації, дисемінації та архівації інформації в соціальних системах, які є особливо чутливими до впливу як внутрішніх, так і зовнішніх інформаційних потоків. Саме через цю вразливість ці процеси організовуються та контролюються на рівні всіх суспільств.

Державна інформаційна політика повинна визначати основні принципи для вирішення ключових завдань соціального розвитку. Серед основних цілей

— створення єдиного інформаційного простору України, інтеграція в глобальний інформаційний простір, а також забезпечення інформаційної безпеки громадян, суспільства та держави.

В сучасному контексті, інформаційна політика виступає інструментом для гарантування безпеки на персональному, суспільному, державному та міжнародному рівнях. У численних країнах та міжнародних організаціях діють спеціалізовані структури, відповідальні за впровадження та реалізацію інформаційних політик.

В контексті реалізації інформаційної політики функціонують потужні структури як у авторитарних режимах, так і в демократичних системах управління. Ці структури сприяють адміністративній підтримці та концептуальній структуризації інформаційної політики, що має ключове значення для адресації значущих національних і міжнародних завдань.

Особливо важливими аспектами інформаційної політики під час військових конфліктів є забезпечення балансу між інтересами суспільства, забезпеченням доступу до об'єктивної та своєчасної інформації, а також дотриманням вимог конфіденційності. Виклики в умовах ведення воєнних дій вимагають взаємодії збройних сил та інших мілітаризованих формувань в контексті контрнаступу проти агресії.

Влада проявляє себе через комунікативно-інформаційні процеси. Отже, управління соціальними процесами державою потребує наявності різноманітних джерел та потоків інформації, які об'єднують соціальні потреби, інтереси та погляди учасників соціально-політичного процесу.

Це допомагає покращити ефективність реалізації політики державних органів та визначає характер їх взаємодії з громадянським суспільством. Взаємодія між державними інституціями та засобами масової інформації залежить від політичної ситуації та особливостей взаємин між громадянським суспільством і владою в конкретному історичному контексті.

У контексті демократичної політичної системи, засоби масової інформації активно виконують роль автономної структури, яка гарантує

реалізацію механізму зворотного зв'язку у складних політичних системах, сприяючи більш ефективній комунікації між суспільством і державою.

Стійкість та міцність соціальної системи залежить від того, наскільки узгоджено працюють органи державного управління та медіа, які забезпечують взаємозв'язок між громадянським суспільством та державою.

Воєнна агресія і провокаційна відомча політика представники конфліктуючої сторони, спрямовані на поширення переконань щодо нестабільності та загрози погіршення соціально-економічної ситуації, що сприяє зміцненню негативних політично-ідеологічних факторів, які ставлять під загрозу національні цінності, ідеали та традиції, руйнують структури соціалізації особистості та створюють загрозу безпеці людей, суспільства і держави. [13].

Перелік законодавчих та підзаконних актів, що визначають базові засади впровадження медіа політики, включає в себе такі акти, як:

1) Закон України «Про доступ до публічної інформації», який регулює процеси публікації та поширення певних категорій інформації в Інтернеті операторами контенту, а також права користувачів на активний та пасивний доступ до цієї інформації.

2) Закон України «Про основні принципи забезпечення кібербезпеки України», націлений на встановлення правових та організаційних основ для захисту інтересів особи, громадян, суспільства та держави, а також національних інтересів України в кіберпросторі, визначаючи ключові цілі, напрямки та принципи державної політики у сфері кібербезпеки України.

3) Закон України "Про боротьбу з тероризмом" встановлює обмеження на розповсюдження інформації, зокрема, забороняє поширення через засоби масової інформації або інші канали матеріалів, що пропагують або виправдовують тероризм, а також тих, що містять заклики до опору або підтримки осіб, які чинили опір під час проведення антитерористичних операцій [14].

Цей наказ регламентує та встановлює порядок взаємодії з акредитованими представниками засобів масової інформації під час введення воєнного стану. У ньому визначено перелік інформації, розголошення якої може загрожувати безпеці дій Збройних Сил України та інших складових сил оборони, а також негативно вплинути на виконання завдань під час воєнного стану. Також вказано на правила роботи журналістів у зоні бойових дій, що є важливими для управління цим процесом.

У часи дії правового режиму воєнного стану встановлено заборону на розповсюдження інформації, що стосується таких аспектів як наймання інформацію про військові частини (підрозділи) та інші військові об'єкти, що знаходяться в зонах виконання бойових (спеціальних) завдань, включаючи географічні координати їх розташування; чисельність особового складу підрозділів; наявність зброї, бойової техніки, матеріально-технічних засобів, їх технічний стан та місцезнаходження; діючі або заплановані військові операції (бойові дії); характеристики військових частин (підрозділів), їх форми, тактики та методи діяльності за покликанням та інші подібні аспекти.

Ще одним важливим кроком у створенні організаційно-правових основ державної інформаційної політики під час війни став прийняття Закону України «Про медіа» від 13 грудня 2022 року No 2849-IX. Цей закон має на меті забезпечення права на свободу вираження поглядів, доступ до різноманітної, достовірної та оперативної інформації, підтримку плюралізму думок і вільного поширення інформації, захист національних інтересів України та прав користувачів медіа-сервісів, а також регулювання медійної діяльності згідно з принципами прозорості, справедливості та неупередженості.

На жаль, сьогодні законодавче регулювання не охоплює таку важливу складову діяльності ЗМІ, як «журналістське розслідування». Питання, пов'язані з публікацією матеріалів, що висвітлюють можливі порушення прав і свобод громадян, корупційні дії або підозри щодо діяльності посадових осіб, є надзвичайно важливими.

Це набуває особливої актуальності в умовах інформаційних протистоянь і воєнного конфлікту з агресором. Журналістське розслідування передбачає детальний аналіз фактів, подій і досліджень з метою встановлення обставин, пов'язаних з конкретними ситуаціями.

Український науковець О. Глушко пояснює, що журналістське розслідування є жанром аналітичної журналістики, спрямованим на виявлення прихованих причин гострих соціальних проблем, а також на з'ясування справжніх обставин їх виникнення, які часто приховуються владою, політичними та іншими впливовими групами.

Журналістське розслідування є складним, синтетичним жанром, що поєднує елементи проблемної статті, памфлету, нарису, фейлетону, репортажу, рецензії, а також включає документи, листування, протоколи, угоди, архівні та статистичні матеріали. Основним принципом для журналіста, який здійснює розслідування, є прозорість, створення відповідної атмосфери та формування громадської думки стосовно аспектів суспільного життя, що мають потенціал для подальшого розвитку [15].

Для досягнення цієї мети в журналістському розслідуванні застосовуються різноманітні літературно-публіцистичні прийоми та стилістичні прийоми, які спонукали б розумову активність та впливали на емоції людей, спонукуючи їх відповідно реагувати на подію. На підсумку, у воєнних умовах виникає питання: чи є обґрунтованим публічне розголошення результатів "журналістського розслідування" та його обговорення.

У такій ситуації може виникнути напружена конкуренція між урядовими структурами та ЗМІ, що часто набуває антагоністичного характеру, спричиняючи негативний вплив на процеси соціалізації особи, психологічний стан громадян та цілісність соціальної системи, впливаючи на єдність громадянського суспільства і держави.

РОЗДІЛ 2 СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

2.1 Законодавче забезпечення інформаційної безпеки в Україні

Забезпечення безпеки інформаційної сфери та національних інтересів України вимагає пріоритетного розвитку системи регулювання відносин у цій сфері для боротьби з загрозами цим інтересам і організації відповідного правового процесу. Це є необхідним у контексті створення правової держави та розвитку громадянського суспільства, де діяльність державних органів має здійснюватися відповідно до високих стандартів, відповідальних за національну безпеку, повинна здійснюватися відповідно до законодавчих норм, що гарантують права та свободи громадян.

По-перше, правове регулювання у цій галузі спрямоване на встановлення норм і принципів боротьби з загрозами національній безпеці України, засобів їх подолання та погоджувальної політики владних органів.

По-друге, інтеграція України в міжнародне співтовариство створює нові можливості для зміцнення інформаційної безпеки країни шляхом участі у розвитку міжнародного права та створення системи, яка забезпечує захист інформаційного сектору на міжнародному та національному рівнях [16].

По-третє, гарантом права і свободи людини, власних державних інтересів України. Наявність чіткої та прозорої державної політики. Останнім часом велика увага органів державної влади та науковців зосереджується на дискусіях щодо удосконалення правового регулювання інформаційної безпеки в Україні. Це правове регулювання формується через систему норм, які регулюють відносини у сфері інформаційної безпеки та процесу формування цієї системи.

Крім того, сфера публічного адміністрування на медіа просторі включає в себе всі правові норми, які визначають взаємовідносини у цій галузі, правові

відносини, що виникають на підставі застосування правових норм, та відповідні законодавчі акти.

Легітимні норми формують основу для захисту національних інтересів України у сфері інформаційної безпеки та оцінки діяльності держави, суспільства та окремих громадян. Ця основа включає в себе положення міжнародних угод, національне законодавство, укази Президента, розпорядження уряду та нормативні акти органів влади, які регулюють відповідні відносини.

Необхідність правового забезпечення демократичних перетворень у суспільстві та державі вимагає реформування всієї системи законодавства України, оскільки діюче законодавство має значні недоліки. Україні потрібно прийняти багато нормативно-правових актів, які відповідають європейським стандартам [17, с. 50-52].

З урахуванням широкого спектру законодавчої бази, які мають вплив на громадські відносини у сфері медіаційної безпеки України, вважаємо за доцільне провести концептуальний аналіз цих актів.

Під законодавчим контролем інформаційної безпеки України мається на увазі форма правового впливу від держави на суспільні інформаційні процеси з метою їх організації, закріплення та захисту. Сьогодні аналіз є одним з ключових аспектів стратегії адміністративно-правового забезпечення інформаційної безпеки України [18, с. 133].

Нормативно-правове регулювання інформаційної безпеки в галузі прав та свобод реалізується через Конституцію України та такі основні закони, як "Про інформацію", "Про науково-технічну інформацію", "Про Національну програму інформатизації", "Про Концепцію Національної програми інформатизації", "Про поштовий зв'язок" та інші.

Зазначені нормативно-правові документи встановлюють правила для реалізації медіаційної безпеки, високого рівня конфіденційності, конспірації, державних таємниць, захисту конфіденційної інформації та ресурсів з метою втілення принципів безпеки особистості, держави і суспільства [19, с. 55-56].

Існує чіткий пріоритет у якості законодавчих та підзаконних актів, спрямованих на регулювання інформаційно-технічної безпеки в сфері інформаційно-психологічної та правової безпеки, що пов'язано зі швидким розвитком інформаційних технологій та потребою швидко реагувати на зміни стандартів.

Одним з головних недоліків юридичного регулювання інформаційної безпеки в Україні є фрагментарність його в різних нормативно-правових актах різної юридичної сили, де важливі проблеми зафіксовані в різних документах.

Для забезпечення ефективної інформаційної безпеки України критично важливо врегулювати проблему неузгодженості нормативно-правових актів, які не відповідають чинній Конституції. Національне інформаційне законодавство має виправити декларативний характер норм та надати чіткі шляхи їх виконання, оскільки відсутність конкретного тлумачення правил призводить до низького рівня їх реалізації у сфері інформаційної безпеки.

Наявність неоднозначних, абстрактних понять та відсутність базових дефініцій є джерелами загроз для інформаційної безпеки держави. Через аналіз нормативно-правових актів у цій сфері можна зробити висновок стосовно критичної потреби у реформуванні законодавчої бази.

В.А. Ліпкан стверджує, що забезпечення інформаційної безпеки України є важливим елементом державної безпеки і є ключовим для формування основних знань і уявлень про загальний стан безпеки країни. Рівень розвиненості, якість функціонування та безпека інформаційного середовища, а також рівень і якість нормативно-правового забезпечення цих процесів визначають нормальне функціонування суспільства.

Законодавство про інформацію спрямоване на підтримку державної інформаційної політики, що забезпечує гарантований рівень національної безпеки в інформаційній сфері, розвиток інформаційних технологій, засобів захисту інформації, запобігання монополізму, запобігання розробці деструктивних технологій для впливу на людей, захист авторських та суміжних прав тощо.

Збереження інформаційної безпеки є ключовим аспектом в усій комплексній забезпеченні потреб людини, держави і суспільства. Основною метою цього процесу є захист важливих суб'єктів інформаційних ресурсів та законних інтересів. Інформаційна безпека виявляє свою сутність через реалізацію у практичній діяльності, наукових дослідженнях та нормативно-правових документах.

Зараз відбувається процес розробки стратегій для забезпечення національних інтересів та безпеки в інформаційній сфері. Ціль полягає в забезпеченні інформаційної безпеки шляхом впровадження єдиної державної політики з питань національної безпеки, включаючи впровадження заходів економічного, політичного та організаційного характеру, що відповідають загрозам та ризикам національних інтересів особистості, суспільства та держави у сфері інформації.

Щоб забезпечити належний рівень національної безпеки в інформаційній сфері, розробляється система правових норм, яка регулює відносини в цій області, визначає основні напрямки діяльності органів державного управління, формує або перетворює органи та сили для забезпечення інформаційної безпеки і встановлює механізми контролю та нагляду за їх діяльністю [20, с. 5-6].

Необхідно відзначити слова В.А. Ліпкана щодо недопустимості обмеження функціонування системи забезпечення інформаційної безпеки лише законодавчими актами. Формування елементів системи забезпечення інформаційної безпеки ще не є завершеним процесом.

Проблема полягає в недостатній структурі системи національної безпеки і нечіткій національній політиці, що також впливає на політику в інформаційній сфері. Недостатня ефективність нормативно-правового регулювання цих процесів негативно впливає на управління державою в даній сфері [21, с. 21-27].

В Україні є недоліки у законодавчій базі щодо забезпечення інформаційної безпеки. 11 січня 2011 року Верховна Рада України прийняла

за основу проект Закону України "Про Концепцію державної інформаційної політики України", який був представлений Кабінетом Міністрів України [22].

У тексті цього закону зазначено: "Ця Концепція визначає мету, принципи, пріоритетні завдання та основні напрями діяльності держави у сфері розвитку інформаційної сфери, включаючи систему виробництва, використання ресурсів та регулювання суспільних відносин, пов'язаних з отриманням, використанням, поширенням та зберіганням інформації".

Це лише один аспект державної інформаційної політики, який розглядається розробниками документа незалежно від завдань інформаційної підтримки особи, суспільства, держави, внутрішніх та зовнішніх політичних цілей [23].

Основи інформаційної безпеки та розуміння інформаційної безпеки в цій галузі зазвичай поділяються на різні методології, які включають наступні основні аспекти. Доступ до концепції інформаційної безпеки складі розглядається через призму універсального доступу як предмета керування.

Різноманітні стратегічні плани безпеки, включаючи ті, що стосуються інформаційної сфери, отримали визначене юридичне затвердження в рамках парадигми "безпека як захист від загроз". Ця парадигма відображена у Концепції національної безпеки України, прийнятої Верховною Радою України у січні 1997 року, та у Законі України "Про основи національної безпеки України", прийнятому влітку був прийнятий у 2003.

Зараз зрозуміло, що для вирішення проблем в області безпеки необхідно змінити парадигму концепції безпеки та впровадити функціональний підхід до забезпечення інформаційної безпеки. За моделювання загроз національній безпеці в інформаційній сфері та розробку заходів захисту відповідають окремі державні органи.

Інформаційна безпека включає в себе всі аспекти національної безпеки і є відповідальністю всіх суб’єктів владних повноважень України. Лише за допомогою універсального методу можливо використовувати наявний інтелектуальний, організаційний та матеріально-технічний потенціал в

інтересах інформаційної безпеки, забезпечуючи співпрацю та координацію між міністерствами та відомствами.

Необхідність зміни парадигми концепції інформаційної безпеки випливає й із правової норми Основного Закону України, відповідно до якої інформаційна безпека віднесена до найважливішої функції держави, справи всього українського народу [24, с. 112-122].

У процесі розширення міжнародного співробітництва важливо розглядати захист інформаційних ресурсів України як невід'ємну частину всієї системи захисту інформації, яка є ключовою складовою інформаційної безпеки можна охарактеризувати як сукупність заходів, які забезпечують право на доступ до інформації та свободу її використання, охорону інформації та прав власності на неї, а також захист від дезінформації та пропагандистського впливу.

Методологія побудови системи забезпечення інформаційної безпеки та її практичне вирішення доводять, що ефективність будь-якої підсистеми залежить від результативності всієї системи, до якої вона належить. Тобто, для ефективного удосконалення системи забезпечення інформаційної безпеки в контексті міжнародного співробітництва необхідно створити дієву загальну систему інформаційної безпеки, яка є важливою частиною національної безпеки України.

Інформація та інформаційна сфера вважаються ключовими факторами у всіх сферах життя та діяльності соціальної системи, зокрема вони впливають на політичну, економічну, соціальну, оборонну і інші складові національної безпеки.

Зазначається, що потреби до інформаційної безпеки повинні бути визначені на всіх рівнях законодавства, включаючи конституційне законодавство, загальні закони, закони про управління державними системами, спеціальні та відомчі правові акти. До даної структури входять:

Блок № 1 цієї структури -законодавчою базою є Конституція України, яке включає норми, пов'язані з питаннями інформатизації, інформаційної безпеки тощо, які є важливими складовими цього.

Другий блок включає загальні закони і кодекси, що охоплюють такі питання, як власність, надра, земля, права громадян, громадянство, податки, антимонопольна діяльність та інші, які також містять норми права з галузі інформаційного права.

Блок № 3 складається із законів про систему керування. Ці норми стосуються окремих секторів господарства, економіки, системи державних органів і визначають їх статус, включаючи положення щодо забезпечення інформаційної безпеки. Вони повинні гарантувати виконання обов'язків щодо формування та оновлення інформаційної безпеки кожним органом, що має значення для загальнонаціонального інтересу.

Четвертий блок об'єднує специфічні закони, що регулюють окремі сфери відносин, галузі господарства та процеси, зокрема Закон України "Про інформацію" та інші. Цей комплект законодавчих актів становить основу спеціалізованого законодавства для правового регулювання інформаційної безпеки.

П’ятий блок – підзаконні нормативні акти, що регулюють забезпечення інформаційної безпеки. Шостий блок – законодавство України, яке визначає відповідальність за порушення у сфері інформаційної безпеки. На нашу думку, правову основу забезпечення інформаційної безпеки України повинні складати Конституція України, Концепція інформаційної безпеки України, закони України, міжнародні угоди, що отримали схвалення Верховної Ради України, а також підзаконні нормативно-правові акти, видані для їх виконання.

Варто зазначити, що ця сфера суспільних відносин регулюється понад 30 законами. До третього блоку нормативно-правового забезпечення інформаційної безпеки слід віднести:

- загальнодержавні та міжвідомчі напрями політики інформаційної безпеки, що реалізуються відповідними суб'єктами у межах їх компетенції;

- захист прав, свобод і законних інтересів особи, суспільства та держави.

- забезпечення інформаційного суверенітету;

- розробка та реалізація державної інформаційної політики, а також підвищення її значущості у забезпеченні загальної інформаційної безпеки;

- гарантування безпеки функціонування всіх компонентів національного інформаційного простору та інтеграція цього простору в глобальну інформаційну мережу;

- створення єдиної системи захисту та технічної охорони інформації обмеженого доступу, що підлягає державному контролю;

- забезпечення безпеки інформаційно-телекомунікаційних систем, мереж зв’язку та безпечного використання Інтернету.

- захист національних інтересів у рамках міжнародного співробітництва;

- прогнозування ризиків, пов’язаних з внутрішньою та зовнішньою політикою держави, соціально-економічним розвитком і державним будівництвом;

- виявлення потенційних і реальних інформаційних загроз, викликів і небезпек;

- оперативне реагування на негативні інформаційні фактори, виявлення, попередження та нейтралізація джерел внутрішніх і зовнішніх загроз;

- участь у двосторонніх і багатосторонніх механізмах забезпечення міжнародної інформаційної безпеки;

- забезпечення координації, контролю та загальнодержавного управління у сфері реалізації політики з інформаційної безпеки та оцінка її ефективності.

Особливе нормативно-правове регулювання у галузі інформації може бути виражено шляхом сукупності законів. Одним з ключових документів цього комплексу є Основний Закон "Про інформацію", який визначає основи правового регулювання всіх ключових спектрів медіаційної діяльності: цей

закон встановлює можливості людей на доступ до інформації та закріплює правові принципи інформаційної діяльності.

Серед інших важливих законодавчих актів у цій області можна відзначити: "Про інформацію", "Про захист інформації", у рамках державної політики забезпечення інформаційної безпеки в Україні важливою частиною є концепція інформаційної безпеки, а також закони, які визначають заходи щодо захисту інформації в різних сферах життєдіяльності особистості, суспільства та держави, зокрема у політичній сфері економічних, оборонних, правоохоронних, соціально-гуманітарних, науково-технічних, екологічних та інших аспектах.

Також важливе значення мають підзаконні нормативні акти, які регулюють взаємодію органів державної влади та координацію діяльності у сфері захисту інформації [25, с. 68-77].

2.2 Інноваційні методи забезпечення інформаційної безпеки

Варто відзначити, що закон України "Про основи національної безпеки України" встановлює дев'ять сфер, у яких необхідно забезпечувати національну безпеку: зовнішньополітичну, державну, економічну, соціальну та гуманітарну, військову, Забезпечення безпеки нації охоплює заходи, спрямовані на охорону державного кордону, внутрішньої політики, екології, науково-технологічного та інформаційного секторів.

Відповідно, інформаційна безпека є невід’ємною частиною національної безпеки. Закон визначає основні функції системи, які необхідно виконати для забезпечення національної безпеки в усіх вищезазначених сферах. Конкретизація цих функцій, враховуючи особливості інформаційної сфери, дозволяє визначити основні завдання системи забезпечення інформаційної безпеки України.

Національний банк, Державна податкова служба, Державна митна служба, Фонд державного майна та інші центральні і місцеві органи виконавчої влади активно приймають і швидко змінюють нормативні правові акти. Однак нестача чіткого правового регулювання у сфері інформаційних правовідносин ускладнює впровадження суттєвих змін у відносинах у суспільстві.

Відсутність взаємопов'язаних заходів і теоретичних розробок в галузі забезпечення інформаційної безпеки призводить до численних перешкод для повноцінної реалізації державою своїх зобов'язань щодо забезпечення інформаційної безпеки, яка є ключовою складовою національної безпеки [26, с. 328].

Існує нагальна необхідність у розробці єдиного всеохоплюючого законодавчого акта, що гарантував би:

- розробка стратегії реалізації державної політики у сфері інформаційної безпеки;

- формування організаційно-правових механізмів для забезпечення інформаційної безпеки;

- визначення правового статусу учасників інформаційних відносин та встановлення їх відповідальності за дотримання національних норм у цій сфері;

- розробка системи навчання та підготовки кадрів, які працюють в галузі інформаційної безпеки.

Організація гарантування та реалізації інфо безпекивикористовує різноманітні підходи, засоби і техніки, які узагальнено у методах. Метод передбачає виконання певної послідовності дій на основі конкретного плану. Ці підходи можуть бути значною мірою різноманітними і змінюватися в залежності від конкретної галузі діяльності та області застосування.

Серед важливих методів оцінки рівня інформаційної безпеки включає методи опису та класифікації. Для ефективного захисту системи управління

важливо спершу описати, а потім класифікувати різні загрози, ризики та виклики, а також розробити систему заходів для їх ефективного управління.

Різні методи дослідження використовуються для аналізу рівня інформаційної безпеки при активних взаємодіях. Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. Ризики можуть вимагати різних рівнів захисту [27, с. 50-56].

У сфері інформаційної безпеки виділяють фізичний, програмне, управлінське, технічне, рівень використання користувачів, мережеве та процедурне. Фізичний рівень включає в себе організацію та захист інформаційних ресурсів, технологій та систем управління.

На програмно-технічному рівні проводиться ідентифікація користувачів, управління доступом, протоколювання, криптографія, екранування та забезпечення доступності. На рівні програмно-технічних засобів виконуються процеси ідентифікації користувачів, керування доступом, логування, шифрування, захист даних та забезпечення можливості використання.

На технологічному рівні ця стратегія втілюється за допомогою передових автоматизованих інформаційних технологій. На рівні користувача ці заходи спрямовані на зменшення впливу зовнішніх чинників на об'єкти інформаційної безпеки та запобігання негативному впливу соціального оточення на інформацію.

На рівні мережі ця стратегія впроваджується шляхом координації компонентів системи управління, які взаємодіють між собою. На рівні процедур вживаються заходи, які здійснюються персоналом, включаючи управління персоналом, забезпечення фізичної безпеки, збереження продуктивності, реагування на випадки порушень мережевої безпеки та планування реагування на інциденти.

Існує декілька різновидів методів забезпечення інформаційної безпеки:

- однорівневі методи ґрунтуються на одному принципі управління інформаційною безпекою;

- багаторівневі методи використовують декілька принципів управління інформаційною безпекою, кожен з яких вирішує своє завдання. У цьому випадку приватні технології не мають взаємозв'язку між собою та спрямовані лише на конкретні фактори інформаційних загроз.

- комплексні методи представляють собою різнорівневі технології, які об'єднуються в єдину систему з координаційними функціями на рівні організації для забезпечення інформаційної безпеки. Це досягається шляхом аналізу різноманітних факторів ризику з семантичним зв'язком або які генеруються з єдиного центру впливу інформації.

- інтегровані високоінтелектуальні методи - це складні технології, що будуються на потужних автоматизованих інтелектуальних засобах з організаційним керівництвом [28, с. 50-56].

Абстрактні техніки забезпечення інформаційної безпеки використовуються на всіх етапах управління ризиками, включаючи визначення обсягу та контексту інформаційного небезпеки, розробку загальної стратегії та дій у різних сферах життєдіяльності, сприйняття загрози нижчими рівнями управління та виділення необхідних ресурсів для ефективного протистояння загрозі та забезпечення підтримка постійного розвитку ресурсів управління інформацією.

Необхідно відтворити результати аналізу ризиків у конкретну політику безпеки, що враховує національний контекст. Використані методи суттєво залежать від суб'єкта діяльності, об'єкта впливу та поставлених цілей. Для багатьох осіб обмежені можливості забезпечення інформаційної безпеки часто обумовлені джерелом загрози, впливом на громадську думку та втручанням держави, яка зобов’язана вживати рішучих заходів для нейтралізації інформаційних загроз.

Суспільство також застосовує методи соціального регулювання, надаючи підтримку окремим індивідам та громадським організаціям, що постраждали внаслідок виявлення загрози.

Нажаль, в нашій країні не вистачає усвідомлення небезпеки в інформаційній сфері, недостатньо штатів у органах державного управління інформаційною безпекою, а також недостатньої підготовки відповідних фахівців для системи управління інформаційною безпекою.

Дуже важливо застосовувати аналітичні методи для дослідження і вивчення суспільної свідомості в галузі інформаційної безпеки. Наприклад, розуміння необхідності захисту інформації на різних рівнях - індивідуальному, суспільному та організаційному - має на меті подолання поширеного міфу про те, що захист інформації і криптографія ідентичні поняття [29].

Проте таке трактування є наслідком використання застарілих підходів до медіа безпеки, у разі інформаційну безпеку розглядають виключно як захист інформації шляхом шифрування. Сьогоднішнім важливим аспектом інформаційної безпеки є не тільки збереження конфіденційності та секретності інформації, але також забезпечення її доступності, цілісності та захисту від різних загроз.

Тому система повинна бути здатною оперативно реагувати на ці виклики та забезпечувати стабільність у цій сфері. Іншим важливим аспектом захисту інформації є гарантування її цілісності під час зберігання та передачі.

Однією з основних задач захисту є збереження і передача інформації з відсутністю будь-яких змін, яка відома як забезпечення цілісності. Таким чином, хоча конфіденційність інформації завдяки криптографічним методам є важливою, її не можна вважати єдиною вимогою при проектуванні систем захисту даних.

Використання криптографії може призвести до уповільнення передачі даних та обмеження доступу до них, оскільки може призвести до складнощів

у забезпеченні швидкого доступу до інформації. Тому важливо забезпечити конфіденційність інформації у відповідності до її доступності [30].

Управління інформаційною безпекою має базуватися на принципах доступності та захищеності, зокрема система захисту даних зобов'язана забезпечувати доступність та цілісність інформації, а при необхідності забезпечувати конфіденційність.

Захист інформації не залежить лише від технічних заходів. Для ефективного забезпечення інформаційної безпеки важливими є різні моделі та методи оцінки загроз і ризиків. Їх різноманітність є складною та залежить від рівня розвитку конкретної цивілізації, а також від контексту оцінки, наявності повної інформації про фактори ризику, алгоритму розрахунку ймовірності та можливих наслідків.

Наявність конкретних даних дає змогу точно визначити ступінь впливу інформаційної зброї, а також рівень загроз і ризиків. Основними методами аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз та інші. Метою якісної оцінки ризиків є класифікація інформаційних загроз і ризиків за різними критеріями.

Важливим способом забезпечення інформаційної безпеки є використання методу критичних сценаріїв. Ці сценарії досліджують ситуації, коли уявний противник намагається знерухомити систему державного управління та ослабити її здатність ефективно працювати в оптимальних умовах.

Світовий досвід підтверджує, що інформаційні війни стали неот'ємною частиною політики національної безпеки у багатьох країнах. Також варто зазначити спосіб моделювання, який використовується для проведення тренувань з інформаційної безпеки, дозволяє ефективно підготуватися до різних сценаріїв. США мають успішний досвід у цьому напрямку, оскільки одна з провідних корпорацій регулярно організовує оперативно-дослідницькі навчання для моделювання різних видів інформаційних атак під час інформаційних конфліктів [31, с. 190-196].

Метод дихотомії виконує важливу роль у забезпеченні інформаційної безпеки. Для боротьби з інформаційними загрозами необхідно приймати заходи як щодо впливу на джерело загрози, а також на посилення захисту об'єкта безпеки. Це призводить до виділення двох головних областей боротьби. Одна з них визначається загальними джерелами загроз, а інша - заходами забезпечення безпеки об'єкта.

Методи впливу на інформацію за допомогою повідомлень можна поділити на електронні та неелектронні. Цифрові методи використовуються для повідомлень, які зберігаються на електромагнітних носіях та обробляються комп'ютерною технікою. Вони включають у себе дії знищення, спотворення або копіювання повідомлень і можуть бути виконані тільки з використанням відповідної технічної та програмної бази.

Методи впливу на інформаційну інфраструктуру можна поділити на інформаційні та неінформаційні. Інформаційні методи орієнтовані на порушення процесів формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, а також систем автоматизованої обробки інформації, тим самим запобігаючи завданню шкоди об'єктам суспільних відносин, що підлягають захисту [32].

Слід зазначити, що вибір методів і способів протидії конкретним загрозам та небезпекам інформаційній безпеці є ключовою проблемою і важливою складовою реалізації основних напрямків державної політики в сфері інформаційної безпеки.

У межах цієї проблеми визначаються можливі форми діяльності органів державної влади, що потребує ретельного аналізу економічних, соціальних, політичних та інших аспектів, що стосуються суспільства, держави та особистості, а також потенційних наслідків вибору різних способів реалізації цієї діяльності.

В сучасних умовах ключовим чинником розвитку економіки є наука. Вкрай важливо забезпечити безперервний розвиток науки та наукоємних секторів для сприяння економічному зростанню.

Поняття "наукоємний" вказує на зв'язок з великими науковими дослідженнями або на необхідність глибоких наукових розробок. "Наукоємність" вимірюється як ступінь наукового забезпечення конкретної сфери виробництва, господарства або інших видів діяльності. "Сектор" розглядається як частина національної економіки з визначеними соціальними та економічними характеристиками.

Тому можна стверджувати, що "науково-технічний сектор" представляє собою частину економіки держави, яка включає надання послуг та виробництво продукції, що необхідно тісно взаємодіяти з науковими дослідженнями та потребують активного використання сучасних наукових розробок.

Питання розвитку науково-технічного виробництва є ключовим для будь-якої країни, оскільки його розвиток є важливим для підвищення конкурентоспроможності національної економіки. Однак, особливо гостро це питання виникає для України [33, с. 253-259].

Сьогодні науковий сектор має ключове значення для прогресу країни. Згідно з дослідженнями вчених, цей сектор охоплює такі галузі, як виробництво електронних, електричних та оптичних приладів; інформаційні технології; телекомунікації; робототехніка; мікро- та оптоволоконні технології; астрономія; штучний інтелект; матеріалознавство; виготовлення бпла, зокрема космічних; біотехнології, нанотехнології та генної інженерії; мембранні та квантові технології; фотоніка; наноелектроніка; мікромеханіка; ядерна енергетика; розробка глобальних інформаційно-комунікаційних мереж, нові джерела енергії та матеріалів.

Згідно з даними Євростату та порівнянням за стандартною міжнародною торговою класифікацією SITC, у виробництво науково-технічних продуктів входять: телекомунікаційне обладнання, техніка для автоматизованої обробки інформації, генератори для ядерних, гідро- та вітрових електростанцій, радіоактивні матеріали, фармацевтичні препарати, передові продукти органічної хімії та пластмаси, хімічні речовини для сільського господарства,

турбіни та реакторне обладнання, медичні електронні прилади, напівпровідникові компоненти, інноваційні вироби електромашинобудування, авіаційна та космічна техніка, сучасні оптичні та вимірювальні прилади, зброя та озброєння.

Діяльність наукової галузі значно залежить від якості та доступності необхідної інформації і неможлива без застосування сучасних інформаційних технологій. Тому забезпечення інформаційної безпеки в науковій сфері економіки має стати ключовим напрямом розвитку.

Ми пропонуємо розглядати інформаційну безпеку наукової сфери економіки як ступінь захищеності ключових інформаційних ресурсів від негативних впливів, загроз, пов'язаних з використанням інформаційних технологій, несанкціонованого розповсюдження даних, а також порушень цілісності, конфіденційності та доступності інформації [34].

Реалізація безпечного медіа простору стає дедалі важливішим фактором, оскільки стрімкий прогрес технологій вимагає постійної модернізації систем безпеки. Зниження фінансування інноваційної сфери у майбутньому це може призвести до негативних наслідків, зокрема до відставання у розвитку новітніх технологій та їх впровадженні у виробничі процеси, підприємствах та державних установах.

Це також може призвести до зменшення кількості осіб, які займаються науковою та інноваційною діяльністю, а також до виїзду кваліфікованих спеціалістів за кордон. Нехтування у плані використання застарілих технологій, неефективне регулювання також можуть негативно вплинути на рівень інформаційної безпеки як для індивідуумів, так і для компаній, різних секторів економіки та держави в цілому.

Також важливо відзначити, що кожного року Зменшується кількість організацій, що займаються науковими та науково-технічними розробками. Рівень наукового розвитку безпосередньо залежить від числа підприємств і організацій, які займаються науковою діяльністю.

Згідно статистиці, найбільш значне скорочення виконаних робіт відбувається в галузях технічних та природничих наук, Це може вказувати на недостатнє фінансування, нестачу кваліфікованих кадрів для проведення таких досліджень, а також на відсутність належної зацікавленості з боку держави у цих напрямках. Менш значущі скорочення спостерігаються в галузі суспільних та гуманітарних наук.

Розвиток науки є основним фактором, що сприяє прогресу всього науково-промислового комплексу країни. Тому не менш важливо забезпечити не лише швидкий розвиток самої науки, а й гарантувати інформаційну безпеку у всій сфері науково-економічного сектору, що потребує адекватного фінансування для проведення досліджень, впровадження інновацій та забезпечення необхідного рівня захисту.

З огляду на швидкий розвиток інформаційних технологій та їх інтеграцію в ключові сфери суспільного життя, настане момент, коли потрібно буде перейти від захисту інформації до забезпечення інформаційної безпеки. В умовах сучасної науки інформаційна безпека виступає як важливий елемент, що впливає на рівень розвитку науки і є показником ефективності використання технологій та новітніх наукових досягнень [35].

Однак велика кількість українських наукових розробок і технологій, які здатні конкурувати з міжнародними, не отримує подальшого впровадження в Україні через неефективне регулювання інноваційної діяльності, обмежене фінансування та, у результаті, повільне впровадження технологій.

Значення та складність питання інформаційної безпеки полягають у тому, що інформація є основним елементом у всіх сферах діяльності. Ефективність та конкурентоспроможність розвитку науково-технічного сектору загалом і сектору економіки зокрема залежать від раціонального і ефективного управління інформацією, а також, що найважливіше, її безпекою.

Перевищення інформаційної безпеки в галузі наукових досліджень та науково-технічного сектору, державна підтримка в науці, актуальних наукових дослідженнях та розробках, законодавче регулювання у сфері науки

сприятимуть зростанню державної економіки та підвищенню позицій на міжнародному ринку [36].

2.3 Застосування кіберзаходів та кіберзахисту в Україні

У останні часи спостерігається зростання кількості різноманітних видів кібератак: Перешкоди у наданні електронних послуг, блокування роботи державних установ, фішингові атаки через електронну пошту, кіберзлочинність, порушення цілісності та конфіденційності даних, інформаційно-психологічний тиск на громадян, кібертероризм, кібершпигунство, інформаційне проникнення в національний інформаційний простір, блокування діяльності або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки.

Україна впровадила широкий спектр заходів для забезпечення готовності забезпечувати кібербезпеку та відстоювати агресію в онлайн просторі шляхом розв'язання стратегічних, правових, політичних, технічних та організаційних проблем.

Важливою складовою захисту будь-якої країни є її стратегія кібербезпеки. Україна впровадила свою стратегію у січні 2016 року, в якій кібербезпека є одним з основних пріоритетів у забезпеченні національної безпеки. Деталі виконання цієї стратегії зображені у річних планах уряду, які містять заходи для запобігання та реагування на можливі кібернапади з метою створення ефективної системи кібербезпеки у країні. Щоб забезпечити координацію та моніторинг робочої ефективності різних учасників у сфері кібербезпеки, а також функціонування відповідних державних служб, яким відведено конкретні обов'язки з виконання вимог кібербезпеки.

Запроваджено механізм керівництва та організовано діяльність Національного координаційного Центр кібербезпеки при Раді національної

безпеки і оборони України, який безпосередньо координує взаємодію між різними державними органами в разі кібератак і кіберінцидентів в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури, з метою підвищення ефективності управління та реалізації державної політики у сфері кібербезпеки в рамках Стратегії кібербезпеки України.

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) здійснює координацію заходів у галузі кібербезпеки, включаючи боротьбу з кіберзлочинністю, захист критичних інформаційних об'єктів та розробку й впровадження державної політики з кіберзахисту державних інформаційних ресурсів [37].

Державна служба спеціального зв'язку та захисту інформації України здійснює організаційно-технічні заходи для запобігання, виявлення та реагування на кіберінциденти і кібератаки, а також для мінімізації їхніх наслідків. Крім того, ДССЗЗІ координує діяльність урядової Команди реагування на комп'ютерні надзвичайні події України та Державного центру кіберзахисту, який реалізує організаційно-технічну модель кіберзахисту в рамках національної системи кібербезпеки.

Потрібно зазначити, що в Україні після 2014 року законодавство у сфері кібербезпеки зазнало суттєвих змін. На 2019 рік була створена законодавча база для забезпечення кібербезпеки держави, зокрема, затверджено Доктрину інформаційної безпеки України, закони України «Про основні засади забезпечення кібербезпеки України» 2163-VIII, «Про національну безпеку України» 2469-VIII, «Про інформацію» 2657-XII (редакція від 01.01.2017 р.).

Також інші нормативно-правові акти, такі як: «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР (редакція від 19.04.2014 р.), «Про електронні довірчі послуги» 2155-VIII (набрав чинності 07.11.2018 р.), «Про захист персональних даних» 2297-VI (редакція від 30.01.2018 р.) тощо. Низка відповідних положень щодо кібербезпеки закріплена в указах президента, зокрема: «Про Концепцію розвитку сектора

безпеки і оборони України» (№ 92/2016 від 14.03.2016 р.); «Про стратегічний оборонний бюлетень України» (№ 240/2016 від 06.06.2016 р.), «Про Національний координаційний центр кібербезпеки» (№ 242/2016 від 07.06.2016 р.) тощо.

Закон "Про основні принципи забезпечення кібербезпеки України" визначає основні об'єкти кіберзахисту, які складають критичну інфраструктуру держави. Він закріплює термінологію в галузі кібербезпеки на найвищому рівні, регулює принципи забезпечення кібербезпеки, а також національну систему кібербезпеки. Закон визначає державне і приватне партнерство в цій сфері, встановлює відповідальність за порушення законодавства та контролює законність заходів з кібербезпеки в Україні [38].

Для зміцнення міжнародного співробітництва і гармонізації нормативних актів у галузі кібербезпеки. Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та інші міжнародні угоди, що відповідають стандартам ЄС та НАТО.

Завдяки підтримці трастового фонду НАТО були створені ситуаційні центри при СБУ та ДССЗЗІ, які мають завдання виявлення, запобігання та нейтралізації кібератак на Україну. Це призвело до запровадження Національного контактного пункту формату 24/7 в Національній поліції України для реагування та обмін даними щодо кіберзлочинів.

Уряд України активно співпрацює на міжнародному рівні для реагування на кіберінциденти, зокрема для зміцнення захисту критичної національної інфраструктури з кібербезпеки, застосовуючи сучасний міжнародний досвід та інноваційні алгоритми для реагування на кібернапади.

Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та інші міжнародні угоди, що відповідають стандартам ЄС та НАТО. Завдяки підтримці трастового фонду НАТО були створені ситуаційні центри при СБУ та ДССЗЗІ, які мають завдання виявлення, запобігання та нейтралізації кібератак на Україну.

В рамках співпраці з міжнародними організаціями щодо реагування на кіберінциденти Україна взяла участь у Форумі команд реагування на інциденти інформаційної безпеки FIRST, що об'єднує різні групи CERT з європейських країн.

Розвідувальні ініціативи в галузі кібербезпеки потребують усебічної обізнаності всіх зацікавлених сторін з факторів ризику, навичок і засобів їх вирішення, а також відповідних заходів для запобігання кібератак. Україна активно співпрацює з провідними організаціями для підвищення обізнаності комерційних підприємств та неприбуткових організацій у галузі кібербезпеки на різних рівнях [39].

CERT-UA-Derzhavnyi Tsentr Zakhystu Informatsiino-Telekomunikatsiinykh System (DTSZITs) ДССЗЗІ зосереджується на виявленні кіберінцидентів та оперативному реагуванні на них. На своєму сайті продемонструє уразливості стандартних оборонних механізмів даних, надає рекомендації щодо мінімізації ризиків та надає технічну допомогу у подоланні наслідків кібератак. Команда взаємодіє з іншими групами країн-членів CERT для аналізу причин та обставин кіберінцидентів, що виникають у критичній інформаційній інфраструктурі.

Згаданий нормативно-правовий акт «Про основні засади кібербезпеки України» погоджує функіонал команди на юридичному рівні. Згідно з цим Законом, CERT-UA та Центр реагування на кіберзагрози будуть координувати заходи, спрямовані на швидку (кризову) реакцію на кібератаки та кіберінциденти, а також будуть запроваджувати контрзаходи з метою мінімізації вразливості систем зв'язку.

У різних українських вищих навчальних закладах поширюються освітні програми з кібербезпеки на бакалаврському, магістерському та професійному рівнях. Це свідчить про значні політичні, економічні та соціальні зусилля у зміцненні кіберстійкості, націлених на розвиток кібербезпеки національних можливостей навіть у зустрічі з численними кібератаками.

Аналіз показує, що при продовженні та активізації трансформації протягом двох-трьох років можна досягти стійкого рівня кіберстійкості, де безпека буде вбудована у структуру організацій як їхній стандартний процес.

Забезпечення кібербезпеки можливе лише через комплексне та постійне застосування організаційно-правових і технічних заходів захисту на різних етапах впровадження. Розглянемо політичні, технічні та організаційні аспекти, вирішення яких є необхідним для інтегрованої боротьби з кіберзагрозами.

Серед Завдань, що постають перед державними установами України у забезпеченні інформаційного та цифрового суверенітету, входять: автоматизоване моніторингування власного інформаційного простору; введення законодавства щодо відповідальності за контент; впровадження законодавства [40, с. 131-138].

Необхідно зосереджуватися на аналізі загроз в кіберпросторі та збирати та поширювати дані про події для більш ефективного реагування. Це повинно здійснюватися регулярно, щонайменше один раз на рік, з метою створення громадських звітів про кіберзагрози та їх своєчасну публікацію на відповідному веб-сайті.

Для розвитку потенціалу сектора безпеки та оборони в галузі кібербезпеки потрібно створити та запровадити ефективні інструменти для можливого реагування на агресію в кіберпросторі. Це може стати засобом стримування військових конфліктів і загроз у кіберпросторі.

Міжнародне співробітництво важливо для підвищення взаємної довіри та роботи над спільними підходами у протидії кіберзагрозам. Країна повинна активізувати зусилля у спільних міжнародних проектах для нарощування кібернетичного потенціалу та запобігання незаконному використанню кіберпростору у воєнних цілях.

Дослідження вказує на те, що ефективна захист кібербезпеки потребує комплексних заходів і координації на державному, регіональному та міжнародному рівнях для попередження, підготовки, реагування та

відновлення після інцидентів з боку державних органів, приватного сектору та громадянського суспільства.

З огляду на сучасні суспільно-політичні та інформаційні виклики, визначення політичних, науково-технічних, організаційних і просвітницьких напрямів розвитку ефективної системи кіберзахисту в рамках комплексної протидії кіберзагрозам сприятиме створенню дієвого механізму для запобігання загрозам у кіберпросторі, оперативного реагування на зміни в цифровому середовищі, а також розробці та впровадженню ефективних інструментів для відповіді на агресію у кіберпросторі, яка може використовуватися як стратегія стримування [41, с. 776].

РОЗДІЛ 3 ВПЛИВ ВОЄННОГО СТАНУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ УКРАЇНИ

3.1 Особливості впливу воєнного стану на інформаційну безпеку в Україні

Національна безпека визнається ключовим компонентом суверенної держави. Для країни, яка недавно відновила свою незалежність, важливо гарантувати свій суверенітет у всіх сферах.

У наш час інформаційний простір відіграє важливу роль як основна база даних і джерело воєнно-стратегічної інформації. Умови повномасштабної збройної агресії підкреслюють значення інформаційної безпеки.

Інформаційна безпека відноситься до ступеня захищеності інформаційного середовища в суспільстві, організації чи особи від негативних наслідків маніпулювання інформацією, які можуть виникнути в результаті умисних, несанкціонованих або неумисних втручань.

Така безпека держави визначається рівнем захищеності основних сфер життєдіяльності, таких як економіка, наука, техніка, управління, військова справа, громадянська свідомість тощо, від потенційно шкідливих впливів у сфері інформації [42, с. 725].

У сучасних умовах військово-політичної сфери недоцільно і складно ігнорувати важливість інформації як засобу впливу, яка фактично може використовуватися як зброя. Інформація може бути ефективним інструментом у перемозі війн та розв'язанні політичних криз, і при цьому не потрібно використовувати фізичну силу.

Тактика такого впливу є характерною для гібридних воєн, де військовий аспект є лише однією зі складових частин. Важливо відзначити, що у ситуаціях, коли інформація використовується для маніпулювання громадською думкою через фізіологічні та психологічні методи, недостатня

рівень інформаційної грамотності призводить до зниження здатності особистості критично сприймати інформацію. У таких випадках важливо аналізувати та оцінювати отриману інформацію, оскільки здатність до формування власної думки може бути практично втрачена.

За воєнної безпеки держави розуміється заходи, спрямовані на захист життєво важливих національних інтересів з використанням військової сили для запобігання воєнним загрозам та агресії.

Основною метою воєнної безпеки є уникнення воєнних конфліктів, і рівень безпеки служить як міра ефективності воєнної політики країни. Тому для забезпечення обороноздатності країни необхідно підтримувати стан, що унеможливлює воєнні конфлікти, відвертає можливу агресію та підвищує готовність оборони для забезпечення стабільності на світовому та регіональному рівнях.

Гібридні методи проведення сучасних воєн створюють надзвичайну важливість забезпечення інформаційної безпеки Збройних сил України. Замість традиційної гарячої війни з військовими конфліктами приходить війна гібридного характеру, яка спрямована на спровокування громадянських війн та створення дезінформаційного хаосу на території ворога.

Для досягнення цієї мети застосовуються різні методи, починаючи від хакерських атак на ключові системи, що забезпечують функціонування держави і закінчуючи маніпулятивною роботою з мас-медіа.

Умови, в яких знаходиться наша країна на сьогодні, заставляють нас переглянути питання національної безпеки з іншого ракурсу. Якщо ще рік тому навколишній світ здавався стабільним, то сьогодні виклики несе значно більшу небезпеку, ніж у мирний час.

У часи війни під загрозою опиняються не лише інтереси держави, але й безпека особистості, суспільства та країни є важливим аспектом захисту прав і свобод особи, оскільки ґрунтується на цілісності даних, доступності інформації, конфіденційності та надійності збереження даних.

Інформаційна безпека охоплює не тільки нормативно-політичні аспекти, але й інституційну сферу, що включає діяльність органів, відповідальних за її забезпечення, а також застосування програмно-технічних засобів. Для гарантування інформаційної безпеки в Україні була затверджена «Доктрина інформаційної безпеки України» Указом Президента України від 25 лютого 2017 року [43].

У військових умовах весною 2022 року рішенням РНБО було ухвалено впровадження єдиної інформаційної політики під час воєнного стану, визнаючи її пріоритетним аспектом національної безпеки. На сьогодні в Україні функціонує Центр протидії дезінформації при РНБО, де можна отримати актуальну інформацію та аналіз подій у цій сфері.

Створення глобального простору значно збільшило загрози, пов'язані з використанням інформаційних методів у рамках стратегічних загроз або глобального тероризму, як у контексті окремих військово-політичних операцій, так і через розвиток їх стратегічного потенціалу загалом. Захист від таких загроз є важливим завданням для Збройних Сил та їхнього персоналу, які перш за все стикаються з методами гібридної війни.

Значення інформації зростає, і її захищеність від злочинних атак стає все більш важливою, а можливості для доступу до неї поширюються. Вміння правильно керувати інформаційними потоками та ефективно їх використовувати стає одним з ключових завдань для військовослужбовців.

Захист інформації Збройних Сил є ключовим елементом національної безпеки. Спеціалісти з безпеки повинні надавати першочергове значення захисту військових інформаційних ресурсів, щоб ефективно протидіяти загрозам.

Для цього необхідно ідентифікувати і класифікувати загрози за джерелами, впливом та рівнем небезпеки. Існують дві основні групи джерел загроз: внутрішні та зовнішні, але іноді можуть спостерігатися комбіновані загрози. Наприклад, зовнішня атака може бути транслювана через внутрішні оператори.

Сьогодні у таких ситуаціях використовуються сучасні електронні засоби для поширення інформації. Додатково, одним з основних джерел інформаційних загроз є напруженість або дестабілізація соціально-політичної обстановки в місцях дислокації Збройних Сил.

Створення штучно напруженої атмосфери, провокування конфліктів із місцевим населенням, а також масові заворушення, спровоковані цілеспрямованим інформаційним впливом, становлять серйозну загрозу для стабільності ситуації у військових частинах та в армії загалом. Протистояти цьому можна лише за допомогою систематичної психолого-просвітницької роботи з особовим складом та активної співпраці з регіональними органами влади для запобігання провокаціям з боку ЗМІ та інших джерел інформаційних атак.

Однією з серйозних загроз є вплив на моральний стан військ через спотворення фактів військової історії, загострення соціальної напруги та спроби втягнути особовий склад у політичні конфлікти. Як правило, такими інформаційними загрозами займаються засоби масової інформації, метою яких є створення напруженої атмосфери.

Іноді взаємодія особового складу з представниками преси може бути засобом спеціальної маніпуляції з наданою інформацією, що в свою чергу може призвести до ослаблення бойового духу військових.

Інколи через такий вплив можуть виникнути не лише психологічні розлади, які можуть призвести до військових злочинів або дезертирства, але й Формування в рядах армії груп, які мають на меті навмисне ослаблення обороноздатності країни, є серйозною загрозою.

Поширення радикального ісламізму може становити величезну небезпеку для інформаційної безпеки армії. Військовослужбовець, який пройшов психологічну обробку, може почати сприймати себе не лише як частину збройних сил, а членом релігійної громади, виконуючи вказівки наставників замість наказів командування.

Такий військовослужбовець може становити значну загрозу для інформаційної безпеки військових частин, особливо в районах, де переважає мусульманське населення. Технічні загрози інформаційного характеру охоплюють як роботу інформаційних систем, що використовуються в армії, зокрема системи управління, так і захист конфіденційної інформації, яка передається через військові канали зв'язку.

Технічні загрози для Збройних Сил можуть варіюватися від навмисного пошкодження систем і крадіжки інформації до помилок, допущених окремими співробітниками. В цьому контексті заходи захисту орієнтовані на підвищення безпеки автоматизованих систем управління та навчання персоналу відповідно до вимог безпеки інформації.

Стандарти безпеки визначаються державними стандартами (ГОСТами) та іншими методиками, але запровадження нових програмно-технічних засобів, які б відповідали сучасним загрозам з боку противника, часто відкладається на практиці. Це затримка обумовлена особливостями системи державних закупівель і становить загрозу для безпеки [44, с. 68-75].

Цей тип нападу включає навмисне пошкодження техніки та ліній зв'язку, яке може статися через неуважність особового складу, місцевих мешканців або внаслідок цілеспрямованих дій ворога. Порушення систем життєзабезпечення військового корабля, спричинене недбалістю чи запланованими атаками, може призвести до загибелі екипажу.

Контроль за збереженням військової техніки вважається одним із найважливіших завдань, яке стоїть перед відповідальними військовослужбовцями. Особливо серйозні проблеми можуть виникнути з інформаційними системами космічних сил або ядерних установок.

Порушення систем управління космічними кораблями через неефективний код, що вбудований в програмний продукт, часто призводить не лише до фінансових втрат, а й до порушення цілісності системи безпеки країни.

Дуже важливо бути усвідомленим загрози надходження недостовірної інформації у систему виявлення можливих атак. Існує ризик вразливості і використання ПЗ внаслідок поширення неправдивої інформації, надісланої зловмисником з обмислом. У минулому, уявлені загрози були майже причиною ядерної війни, хоча зараз цей ризик зменшився, але не зник. Наразі серйозною проблемою є відсутність ефективних правових норм щодо захисту інформації від нових загроз.

Багато явищ в інформаційному просторі ще не класифіковані і не охарактеризовані у законодавчих актах, що ускладнює введення покарання за неправомірну діяльність або створення обставин, за яких можуть виникнути загрози безпечному існуванню медіа простору Збройних Сил. Проте ці напрямки оновлюються, приймаються законодавчі акти, які забезпечують регулювання допустимості використання закордонних технологій у військовій техніці.

З дати оголошення закону «Про введення правового режиму воєнного стану в Україні» були проведені реформи до законодавчих актів, що підлаштовуються до умов збройного конфлікту. Певні реформи охоплюють керування всіма сферами інформаційного простору, встановлення правових обмежень щодо поширення певних видів інформації, яка має суспільно небезпечний характер, а також нормування процесів запису інформації у воєнний період.

Ухвалений Верховною Радою законопроект, що встановлює кримінальну відповідальність за незаконну фіксацію фото- та відеоматеріалів, пов'язаних з Збройними Силами та міжнародною військовою допомогою під час воєнного стану, набув чинності 22 березня 2022 року. Цей закон полегшує проведення слідчих дій, дозволяючи тимчасовий доступ до речей і документів, а також надає слідчим можливість фіксувати комп'ютерні дані під час обшуків.

Уряд України випустив закон, ухвалений 3 березня 2022 року, збільшив відповідальність за виготовлення та розповсюдження незаконної інформаційної продукції. Згідно з цим законодавчим актом, посилено

кримінальну відповідальність за виробництво та поширення заборонених інформаційних матеріалів.

Зовнішні джерела загроз включають у себе потенційні небезпеки, які походять з-за кордону України або країни-партнера. Противник постійно вдосконалює свої інформаційно-психологічні методи для впливу на особовий склад.

Розробка нових видів інформаційної зброї, яка може призвести до збоїв в інформаційних системах або впливу на психіку персоналу, є серйозною загрозою. Експерти вважають, що механізм дії такої зброї базується на використанні ультразвуку, електромагнітних полів та різних типів мікрохвиль.

Існує ймовірність використання медичних та хімічних препаратів для регулювання поведінки військових у мирний та воєнний час не виключено. Такі методи психологічних операцій можуть бути запроваджені у зонах бойових дій.

Засоби психологічної впливової діяльності обговорюються у пресі, але поки що немає офіційних заяв про їх використання. Відомо, що у збройних силах стратегічного супротивника або глобальних терористичних організацій діють спеціальні підрозділи інформаційно-психологічного впливу, але їхні методи вивчаються тільки На рівні науково-дослідних установ розробляються та впроваджуються заходи для боротьби з новими загрозами.

Часто планування та підготовка цілеспрямованого інформаційного впливу відбуваються заздалегідь шляхом ретельної роботи з різними засобами. У військових обов'язки входить вміння класифікувати та ідентифікувати такі загрози, для чого необхідна відповідна підготовка [45, с. 121-128].

Однією з найбільших загроз безпеці є використання соціальних мереж, через які військовослужбовці можуть випадково розголошувати конфіденційну інформацію. Важливим завданням у забезпеченні безпеки держави є виявлення таких загроз і їх своєчасне усунення.

Заходи для захисту інформації та забезпечення безпеки можна поділити на дві основні категорії:

- захист інформаційних систем від шкоди, а також запобігання витоку і перехоплення даних.

- - захист психічного стану особового складу від навмисного інформаційно-психологічного впливу.

Ці заходи повинні реалізовуватися комплексно, з застосуванням сучасних наукових розробок та програмних продуктів. Перша група заходів охоплює:

- захист об'єктів військового розташування та комп'ютерної техніки, що знаходиться в них, від атак з вогнепальної зброї або інших злочинних дій;

- захист систем від віддалених атак зловмисника, зокрема за допомогою встановлення програмних продуктів, які гарантують комплексний захист від вторгнень, наприклад, системи DLP та SIEM.

- безпека конфіденційних відомостей, що стосується державних або військових таємниць, від витоку або навмисного викрадення;

- захист від радіоелектронних атак;

- застосування захищених комп'ютерних моделей та програмного забезпечення, що не піддаються попередньо створеним проблемам у своєму коді;

- створення інструментів для електронної розвідки;

- застосування соціальних мереж для стратегічного поширення дезінформації серед ворога;

- захист систем зв'язку.

Другий набір заходів включає:

- запобігання навмисного психологічного впливу на психіку військових;

- редагування відомостей, яка передається ворожими силами.

Розробка та впровадження цих заходів потребує створення спеціалізованих підрозділів, які зосереджуються на інформаційній безпеці. Морально-психологічне забезпечення військ включає застосування комплексу

заходів блокування, що використовуються в умовах гібридної війни. Наразі існують інститути та аналітичні центри, які фокусуються на розробці різноманітних методик морально-психологічного забезпечення військових. В рамках цих досліджень аналізуються психологічні аспекти та забезпечення безпеки психоенергетичної діяльності.

Для протидії цілеспрямованому інформаційно-психологічному впливу командування Збройних Сил застосовує наступні методи:

- проведення досліджень, орієнтованих на вплив на психіку;

- використання різних видів психологічної роботи з військовослужбовцями та реалізація цілеспрямованих захисних заходів.

Ці дії необхідні для створення надійного захисту від інформаційного впливу та підготовки військовослужбовців до відсічення шкідливої інформації, що спрямована на дестабілізацію їх морально-психологічного стану. Напад противника не повинен підточувати боєздатність військ, їх мотивацію або віру.

Важливо проводити виховну роботу та організовувати відпочинок військовослужбовців. Особливо важливо контролювати тих військовослужбовців, які відповідають за роботу з комунікаційними засобами, автоматизованими системами управління та передачі інформації, оскільки вони можуть стати об'єктами атаки ворога [46, с. 81-85].

Щоб запобігти можливому комплексу заходів потенційного противника, необхідно скористатися атакою для обмеження його можливостей. Це включає в себе такі дії, як:

- введення супротивника в оману стосовно його стратегічних намірів та методів боротьби з загрозами інформаційній безпеці;

- нейтралізація засобів зв'язку та інформаційних систем противника;

- створення фальшивих даних у функціонуванні інформаційних систем супротивника;

- виявлення ключових точок противника на території України та їх знищення.

- отримання секретної інформації про плани супротивника для ослаблення безпеки військ і використання цих даних при формуванні оборонної стратегії;

- застосування психологічного тиску для нейтралізації інформаційних сил противника.

Створення ІПСО вважається важливою складовою оборонної стратегії. Вона має бути розроблена не лише для реагування на загрози, але й для їх передбачення.

Ворожі сили з великим успіхом застосовує інформаційну зброю, що підтверджується досвідом країн, які залучені до військових конфліктів. Інформаційна зброя використовується не лише на фронті, але й в регіонах, де може виникнути дестабілізація.

Місцева інформаційна зброя повинна мати таку саму або ще вищу ефективність. Щоб забезпечити безпеку кожного військового об'єкту, потрібно підходити до цього комплексно, враховуючи можливі ризики.

Держава активно займається вирішенням цих завдань і зміцнює свій оборонний потенціал. Розробка власного програмного забезпечення сприяє запобіганню системним загрозам.

Крім того, канали передачі даних в Інтернеті повинні забезпечувати можливість комунікації без порушення архітектури Всесвітньої мережі, тому на цих етапах важливо гарантувати повну безпеку для користувачів. Відсутність належного контролю за постачальниками та підрядниками може призвести до того, що вони нададуть обладнання, яке дозволяє потенційному супротивнику здійснити віддалений доступ.

В окремих випадках використання таких пристроїв заборонено законом, але технічний арсенал армії ще не повністю оновлений. Значною вразливістю систем автоматизованого управління армії є передача конфіденційної інформації через відкриті канали зв'язку, що іноді можуть бути доступні цивільним фахівцям. Цю загрозу необхідно локалізувати якнайшвидше.

Відповідно до законодавства України, загрози національній безпеці країни визначаються як фактори, явища або тенденції, які заважають або можуть заважати реалізації національних інтересів та збереженню національної цінності [47, с. 334-338].

3.2 Роль інформаційної війни та пропаганди в контексті воєнного стану

Інформаційна боротьба між росією та Україною почалася ще з отриманням Україною незалежності у серпні 1991 року і триває до сьогоднішнього дня. Сучасні експерти відзначають, що починаючи з моменту незалежності, росія проводить систематичну інформаційну пропаганду.

Серед конфліктів між Україною та росією, де спостерігалося велике впливу інформації, зазначити можна територіальний конфлікт, що стався в районі острова Тузла у 2003 році, а також "газові" війни 2005 та 2009 років та інші подібні інциденти. Інформаційна війна була посиленою за правління президента В. Януковича.

Російські медіа розпочали масовану інформаційну кампанію проти Майдану наприкінці 2013 року, яка з часом переросла в збройну агресію. Після введення російських військ до Криму, росія почала активну інформаційну війну проти України. Щороку російська влада витрачала до 4 мільярдів доларів на цю боротьбу.

У 2014 році росія впровадила агресивні плани стосовно України, включаючи посилення Конфлікт в інформаційному просторі. Інформаційна кампанія була спрямована не тільки на підтримку анексії українських територій, але й на надання легітимності цьому процесу.

Головна стратегія інформаційно-психологічних операцій полягала в підриві громадянської ідентичності України та спонукання українців відмовитися від захисту своєї держави. Основною метою було сформувати

уявлення серед громадян України, росії та Європи, що створення або відновлення української держави є неприродним процесом.

Поширювались заяви про "неонацистське панування", яке нібито встановилося після перевороту, а також про необхідність тісної співпраці або об'єднання з російською федерацією для поступового розвитку українського суспільства. росія активно використовувала медіа для поширення різноманітних соціальних технологій, спрямованих проти України, таких як розподіл країни на "народні республіки", створення кримінальних мас, підбурювання до заколотів та захоплення влади в містах, проведення "референдумів", використання "живого щита" та інші методи.

Як зазначають дослідники, ці технології мають певні спільні риси, зокрема загальні цілі, використання стандартних методів, координацію дій в різних містах України, однакову зовнішню символіку та інформаційну підтримку ідеологічного й пропагандистського характеру. Після 2014 року російські ЗМІ застосовували різноманітні методи для виправдання вторгнення росії на українську територію, часто спотворюючи факти та активно поширюючи дезінформацію.

Журналісти маніпулювали фактами та надавали недостовірні інтерпретації. Російські ЗМІ прагнули переконати свою аудиторію, що в Україні панує "хаос і безлад", і що російські війська нібито допомагають зберегти стабільність і захищати російськомовних громадян від так званої "коричневої загрози", яку навіть президент Путін вважав серйозною небезпекою.

З 2014 по 2022 роки пропагандистська машина Кремля активно готувала ґрунт для можливого вторгнення в Україну, формуючи аргументи для виправдання своїх дій на міжнародній арені та створюючи систему блокування інформації від європейського та американського світу для власних громадян.

Усі ці заходи зіграли важливу роль в інформаційній війні, сприяючи формуванню уявлень громадян та військовослужбовців росії щодо проведення

так званих "спеціальних операцій" та процесів "денацифікації і демілітаризації" в Україні [48, с. 23].

Наразі росія проводить активну агресивну кампанію проти України, анексувавши Крим та частину південних і східних регіонів. З початку російського вторгнення 24 лютого 2022 року пропаганда ворога значно посилилась і стала ще більш агресивною.

Основні медіа продовжують поширювати фальшиві новини та пропагандистські матеріали, щоб виправдати свою агресію. Головною метою росії є розпочати повномасштабну війну проти України з метою об'єднання колишніх радянських республік та геополітичного перерозподілу євразійського регіону під контролем столиця країни агресорки.

Дезінформація, що супроводжувала масштабне вторгнення Росії в Україну у лютому 2022 року, сприяла загостренню тривалих інформаційних операцій росії проти України та західних демократій.

З посиленням обмежень на політичну опозицію в росії, дезінформаційні наративи перейшли від пропаганди до історичного ревізіонізму. Це включало, наприклад, наполегливе твердження, що Крим "завжди був російським" після його анексії Москвою у 2014 році, фальшиві звинувачення про наявність неонацистів у українському уряді, а також теорії змови щодо біолабораторій в Україні та США.

Ці зусилля демонструють кілька способів, якими російський уряд та його союзники використовують дезінформацію як інструмент для маніпуляцій, заплутування та ослаблення своїх супротивників. Росія виправдовує свої дії за допомогою стратегії, характерної для тоталітарних режимів, створюючи образи зовнішнього та внутрішнього ворога.

Головним ворогом росія намагається зобразити весь колективний Захід, тоді як внутрішнім ворогом виступає опозиція. Формування образу ворога слугує прикриттям для агресивної політики росії, допомагає "мобілізувати" населення проти уявних зовнішніх загроз, викликає почуття незахищеності та відволікає увагу від внутрішніх кризових проблем.

Ностальгія за радянською добою в колишньому Радянському Союзі визначається як потужний інструмент пропаганди, що використовується для маніпуляції публічною думкою. Цей наратив став ключовою частиною інформаційної стратегії росії, яка була націлена на анексію Криму та початок конфлікту на сході України у 2014 році.

Це було досягнуто переважно за допомогою фільмів та серіалів, які посилюють ідею "великої перемоги" над фашистами та сприяють ностальгії за радянським періодом через обіцянку соціального захисту та стабільності.

Деякі громадяни України також сприймали штучний проект "Новоросія" як відображення реальності їх майбутнього. Однак виявилося, що ці "республіки" були неспроможні у своєму розвитку, оскільки вони могли існувати лише завдяки пропагандистській теорії в інформаційній війні. ІПСО не базуються на жодному підґрунті, а лише посилюють нестабільність та соціальну напругу в Україні.

У місяці серпні 2020 року Держдеп США опублікував доповідь, у якій ідентифіковані п'ять ключових складових системи російської пропаганди та дезінформації [49].

За словами американських експертів, ці елементи включають офіційну комунікацію влади, державну глобальну інформаційну службу, фінансовану урядом, проксі-ресурси (ЗМІ в інших країнах, що мають зв'язки з росією, а також "експертів", які поширюють російські наративи за кордоном), соціальні мережі та кібер-дезінформацію.

Іншим аспектом, на який намагалася вплинути російська пропаганда, є інформаційна боротьба в освіті. Зусилля, спрямовані впливання на молоде покоління є частиною загальної інформаційної агресії проти України. Наприклад, раніше робилися спроби запровадити український підручник з історії, розроблений за участю російських "вчених". Однак ці спроби були зупинені завдяки рішучому опору експертів, українських істориків та педагогів.

Ворожі медіа, як традиційні, так і онлайн, продовжують поширювати міфи про нібито "неонацистів" чи "нацистів" в Україні, які, за їхніми твердженнями, переслідують російськомовне населення країни.

З іншого боку, ворожі медіа сором'язливо ухиляються від вживання слова «війна». Варто зауважити, що в росії за його використання можна отримати покарання у вигляді тюремного ув’язнення на строк до 15 років. Тому російську агресію проти суверенної держави часто прикривають поняттям «спецоперація».

Логічно, що коли ворожі війська нападають на іншу країну, обстрілюючи її міста та спричиняючи загибель цивільних, у тому числі жінок і дітей, це можна кваліфікувати як акт війни та, можливо, навіть як акт тероризму. Спроба заміняти ці терміни призначена для відволікання уваги від справжніх намірів та дій російської влади та для впливу на правдиву обстановку в Україні. Це використання слів має ціль викликати специфічну реакцію у свідомості росіян.

У ході інформаційної війни росія також намагається відобразити українське військове та політичне керівництво як "зрадників", дискредитуючи їх. Одним із яскравих прикладів цього є міф про президента Володимира Зеленського як "втікача".

Окрім того, російська інформаційна кампанія постійно наголошує на негативному ставленні українців, зокрема "нацистів" Західної України, до росіян. Ці аргументи не мають логічного обґрунтування і спрямовані на внутрішнє споживання. Міжнародні організації, оснащені сучасними технологіями, можуть без труднощів відстежувати напрямок бомбардувань і ракетних ударів.

Слід зазначити, що лише за початкові дні війни було зібрано тисячі фактів, що підтверджують злочини російської армії. Ймовірно, такі заяви робляться з метою підтримки внутрішньої аудиторії. Очевидно, що сучасна російська "еліта" частково готова до розриву зв'язків із Заходом, і тому

контроль над настроями власного населення є важливим елементом стабільності режиму Путіна.

Розуміючи, що повний контроль над інформаційним простором у 21 столітті недосяжний, можна визнати, що певна правдива інформація все одно потрапляє в загальний інформаційний простір. У поточній конфлікті між росією та Україною ЗМІ часто не ставлять перед собою завдання об'єктивно інформувати громадян, а скоріше фокусуються на зборі фактів, що в подальшому підтверджують певні погляди [50, с. 67-69].

Головною з ознак інформаційної війни є створення нової реальності через інформацію, де вона використовується для формування конкретного образу світу, і чим швидше ця інформація розповсюджується, тим вищі шанси на її успіх.

Також спостерігається зміна цінностей, зокрема відмова від радянських традицій, що проявляється, наприклад, у відмові від святкування 23 лютого. Окрім того, триває боротьба за спільну історію: історії України та росії стають предметом активної боротьби, включаючи напади на національні символи, воєнну славу та інші важливі елементи.

Усі ці складові свідчать про використання інформаційної війни для маніпулювання свідомістю та переконанням населення, формуванню образів та змінам цінностей. Агресивна кампанія росії проти України особливо вражає своєю інтенсивністю в Інтернет-просторі.

Великий обсяг інформації та її розповсюдження через Інтернет і соціальні медіа відіграють ключову роль у цьому конфлікті. Хоча соціальні мережі вже мали своє значення у попередніх війнах, зокрема на Донбасі в 2014 році, зростання покриття Інтернетом і широке використання соціальних мереж робить цей вплив ще більш потужним.

В Україні високий рівень доступу до Інтернету: 75% населення активно користується мережею, а 89% мають доступ до мобільного зв'язку 3G або вище. Це створює значні можливості для поширення інформації, пропаганди та маніпулювання громадською думкою.

Контроль над інтернет-простором та поширення дезінформації через онлайн-ресурси є ключовими елементами інформаційної війни. Це підкреслює роль Інтернету як потужного інструменту для формування світогляду та впливу на громадську думку в умовах сучасних конфліктів.

Отже, можна підсумувати основні аспекти інформаційної війни росії проти України. В цій війні головним об'єктом впливу є українське суспільство, внутрішня політична ситуація, система влади в Україні, а також окремі політичні та громадські організації, зокрема політичні партії, громадські рухи, релігійні організації та ЗМІ.

Основною метою російської інформаційно-психологічної війни є вплив та дестабілізація українського суспільства «зсередини» через дискредитацію української влади, армії, курсу на європейську та євроатлантичну інтеграцію, а також шляхом загострення соціальних конфліктів та інших деструктивних впливів.

Об'єднання телебачення та пропаганди зумовлене кращим керуванням телевізійною аудиторією порівняно з аудиторією газет або соціальних мереж. Телебачення використовує різні методи впливу на свідомість населення, зокрема створення фейкових новин, повторення інформації, навішування ярликів та інші техніки.

Окрім України та росії, такі країни, як Китай і Білорусь, також активно залучені до висвітлення війни, просуваючи власні наративи та координаційні дезінформаційні кампанії через соціальні мережі. Ці кампанії спрямовані на зменшення відповідальності росії за конфлікт та підтримку антиамериканських і антинатовських настроїв.

Поєднання різних наративів від державних акторів та окремих користувачів соціальних мереж одночасно збільшує роль технологічних платформ у формуванні динаміки конфлікту та може вплинути на його результати [51, с. 17-24].

Маніпулятивні психоінформаційні стратегії, які росія застосовує щодо України, охоплюють кілька основних напрямків і методів, як зазначив дослідник П. Шевчук:

1) спроби підриву міжнародного іміджу України та ослаблення її геополітичного статусу;

2) маніпулювання та спотворення інформації з метою дестабілізації ситуації в Україні та втручання у політику "керованого хаосу";

3) формування та поширення стереотипів, що пропагують ідею меншовартості та другорядності українців, що може призвести до підриву національної гідності.

4) стимулювання самоідентифікації українців в умовах домінування російської мови, культури та традицій, а також пригнічення української мови та культурних особливостей.

Українська дослідниця інформаційної безпеки І. Валюшко виокремила основні підходи до інформаційної агресії проти України, серед яких дезінформація, маніпуляції, пропаганда, диверсифікація громадської думки, психологічний тиск, поширення невизначеності та створення хаосу, кібератаки та інші форми впливу.

Інструменти російської інформаційної війни охоплюють широкий спектр засобів, таких як ЗМІ, "Інтернет-тролі", "боти", текст, відео, аудіо, зображення, меми та інше. Крім того, інформаційну війну можуть вести окремі політичні, громадські та навіть релігійні групи, орієнтуючись на свої конкретні цілі та завдання.

Інформаційна війна росії проти України, що супроводжується широкомасштабним вторгненням, веде до бойових дій, спричиняючи значні людські втрати та руйнуючи перспективні галузі економіки.

Інформаційний сектор став найбільш вразливим у безпековій сфері України, виявивши проблеми як у законодавчій, так і в інституційній сферах. Інформаційно-диверсійний елемент є основним у військовій кампанії на

території нашої країни, а інформаційно-психологічний фактор відіграє ключову роль у ескалації російсько-українського конфлікту [52].

3.3 Міжнародний досвід та кращі практики у сфері інформаційної безпеки під час воєнного стану

У законодавстві США детально врегульовано питання, пов'язані з безпекою інформації в державних комп'ютерних системах, боротьбою з комп'ютерною злочинністю, а також регулюванням балансу між правами громадян на доступ до інформації та захистом конфіденційності їх особистого життя.

Адміністративно-організаційний захист інформаційної безпеки в США орієнтований на координацію заходів із захисту інформації та реалізацію єдиної державної політики у цій сфері, при цьому президент США несе відповідальність за національну безпеку в цілому, а також за інформаційну безпеку зокрема.

Для багатьох очевидно, що як наддержава, США можуть встановлювати інші цілі, ніж Україна у своїй політиці забезпечення безпеки.

Ми повинні усвідомлювати, що не маємо таких самих матеріальних та технологічних ресурсів, як у Сполучених Штатах для забезпечення національної та громадської інформаційної безпеки. Українські фахівці можуть освоїти технологічний досвід, а законодавці мають вивчити ті методи нормативного регулювання інформаційної політики, які зарекомендували себе як універсальні та ефективні в США.

Система кібербезпеки в США є надзвичайно складною та всеохопною. У 2018 році був створений Національний центр кібербезпеки, який відповідає за координацію захисних заходів від кібератак, а також проведення аналізу та моніторингу кіберзагроз у співпраці з різними суб’єктами управління.

У США також розроблено Національну стратегію кібербезпеки, яка ґрунтується на п’яти основних принципах: захист, виявлення, реагування, обмін інформацією та відновлення.

Для реалізації цієї стратегії створено Кібербезпековий центр при Національному інституті стандартів і технологій США, а також інші центри кібербезпеки, які допомагають у розробці стандартів безпеки та методик. Наприклад, Федеральне агентство з кібербезпеки та інфраструктури (CISA) відповідає за захист критичної інфраструктури від кібератак, промислового шпигунства та інших загроз.

Окрім того, у США існують закони, які регулюють захист персональних даних громадян і компаній, гарантуючи високий рівень захисту цієї інформації.

Уряд Китайської Народної Республіки (далі - КНР) виявляє меншу демократію у питаннях, пов'язаних з інформаційною безпекою. В інформаційній політиці Китаю переважають принципи моноцентричних стратегій оборони та наступу.

Інформація для КНР у політичному та безпековому контекстах розглядається як потужний засіб впливу на громадян та для захисту від зовнішніх впливів. Завдяки використанню цієї ресурсної бази Китай здатний здійснювати ефективну інформаційну політику, незважаючи на її демократичні аспекти.

Усі аспекти державної інформаційної політики обумовлені необхідністю захисту національних інтересів шляхом впровадження моделі інформаційного суспільства, що ґрунтується на китайських принципах, та особливостей інтеграції Китаю в глобальне інформаційне середовище. Включення стратегії державної інформаційної політики в урядові програми дозволяє Китаю адаптувати свої політичні принципи до сучасних міжнародних тенденцій розвитку.

Активна участь Китаю в процесах міжнародної регіональної інтеграції формує стратегію державної інформаційної політики, яка полягає в

одночасному входженні до глобальної системи міжнародних відносин і впровадженні національної моделі інформаціоналізму як інструменту модернізації політичної системи Китаю та досягнення потенційного лідерства на регіональному та міжнародному рівнях.

Отже, Китай реалізує власну стратегію інформаційної політики, яка охоплює як внутрішні проблеми країни, так і регіональні та глобальні геополітичні стратегії. Завдяки цій стратегії Китай стає важливим гравцем на світовій геополітичній арені, створюючи серйозну конкуренцію не лише Європі, але й Сполученим Штатам Америки [53, с. 119-132].

У Японії створено Кібербезпековий центр, що займається аналізом кіберзагроз та розробкою рекомендацій для їхнього захисту. Крім того, в центрі регулярно проводяться тренування та навчання з питань кібербезпеки.

Вищевказана країна активно займається забезпеченням своєї інформаційної безпеки, зосереджуючи значні зусилля на цьому питанні. Тамтешні експерти розробляють та вони впроваджують стратегії, спрямовані на запобігання кібератакам та іншим загрозам національній безпеці.

Для цього була створена Національна агенція з питань кібербезпеки (NISC), яка координує заходи для підвищення стійкості японських систем до кіберзагроз. Уряд Японії регулярно укладає угоди з іншими країнами для обміну інформацією та забезпечення безпеки своїх інформаційних мереж. Японія інтенсивно протистоїть зростаючим загрозам кібербезпеки, таким як віруси-шифрувальники та фішингові атаки.

Уряд гарантує безпеку своїх інформаційних систем шляхом встановлення жорстких стандартів зберігання і передачі даних, а також проведення регулярних тестів на стійкість систем. Крім того, він активно працює над забезпеченням безпеки мереж підприємств, які є важливими для економічні сектори країни, зокрема фінансові установи, енергетичні компанії та транспортні системи.

Канада заснувала Національний центр кібербезпеки, який координує національні заходи з кібербезпеки та співпрацює з іншими державами. Крім

того, уряд Канади створив Міністерство безпеки публічної інформації та кібербезпеки.

Забезпечення захисту державних інформаційних систем і мереж для запобігання кібератакам та охорони даних. Канада також активно співпрацює з іншими країнами та міжнародними організаціями, зокрема Північноатлантичного альянсу та ОБСЄ, з метою зменшення загроз кібербезпеці і обміну досвідом [54, с. 37-41].

Уряд Канади підтримує підприємства та громадян у сфері кібербезпеки, забезпечуючи фінансову і технічну допомогу в розробці та впровадженні програм безпеки, а також забезпечення доступу до інформаційних ресурсів і порад з цієї галузі. В цілому, Канада у великому масштабі працює над забезпеченням своєї інформаційної безпеки та боротьбою з потенційними кіберзагрозами, які можуть загрожувати національній безпеці та економіці країни.

Необхідно враховувати висновки, які зробила Н.Ф. Семенова, досліджуючи проблему інформаційної війни росії проти України та способи протидії з боку України, наголошує, що ефективна протидія військовій агресії можлива лише за умови наявності в Україні необхідних засад для боротьби з російською пропагандою.

Вона вважає, що під ІПСО необхідно розуміти всі інформаційні повідомлення з боку росії, російських ЗМІ, включаючи українські російськомовні ЗМІ, які мають негативну ставлення до України. "Для того, щоб успішно протистояти у інформаційній війні та адекватно відповідати російській стороні, потрібно твердо усвідомити, що формат інформаційної війни вже вийшов за межі насильства".

Більшість науковців погоджуються з тим, що інформаційна війна є ключовим інструментом російської агресії проти України, а на даному етапі основною зброєю в цій війні виступає пропаганда.

Метою кожної інформаційної кампанії є сформувати враження у світової та української громадської думки, що урядовий режим в Україні, незалежно

від партії, що перебуває при владі, не є демократичним і підозрюється в корупції чи авторитаризмі.

Вибір сенсаційних тез не має значення, головною метою є принесення шкоди уявленню про Україну як країни, у якій на владі знаходиться режим, який потрібно змінити. У період з 2014 по 2019 роки ця інформаційна кампанія була проведена найбільш агресивно, практично формуючи попередні уявлення для виправдання військової агресії.

Найбільша загроза ефективності протистояння російській агресії полягає у розумінні пропаганди війни у контексті «війни» як міжнародно-правової категорії, яка означає агресію проти держави. Однак Україні необхідно усвідомити, що протистояння відбувається на її власній території, а його учасниками є громадяни України, які отримують фінансування, підтримку та утримання з боку росії. Це не просто концепція війни, але складна ситуація, яку можна класифікувати як «гібридну війну», і яка повинна бути криміналізована [55, с. 31-35].

Однією з ключових причин важливості правових основ для боротьби з російською агресією є постійне порушення росією норм міжнародного права та ігнорування принципів, на яких ґрунтується сучасна система міжнародних відносин. Це призводить до того, що міжнародно-правові стандарти, які встановлюють відповідальність за військову пропаганду, не визнаються росією.

У такій ситуації важливо розробити та впровадити власні правові та організаційні механізми для притягнення осіб, що поширюють військову пропаганду, до відповідальності. Це дозволить істотно збільшити можливості застосування міжнародного правового тиску до росії в рамках боротьби з її агресією проти України.

Ефективніше створювати юридичне, правове та концептуальне забезпечення для трансформації секторів національної безпеки і оборони, а також правоохоронних органів, не лише для протидії та захисту, але й для розробки стратегій щодо повернення територій. Кримінально-правові заходи

протидії пропаганді війни повинні доповнюватися публічно-правовими та економіко-правовими підходами.

Наприклад, у цій постанові, ВРУ зазначає: "Стратегія реінтеграції в Україну тимчасово окупованої території АРК та міста Севастополя: проблемні питання, шляхи, методи та способи" вказується на необхідність реакції України на ІПСО, пониження рівня державної мови, літератури, спотворення національної історії та формування альтернативної, вигаданої російськими ЗМІ, інформаційної картини світу.

Це пов’язано із початком збройної агресії та повномасштабного вторгнення рф на територію нашої держави, та незаконною окупацією Криму і Севастополя, стратегія повернення Криму повинна ґрунтуватися на відновленні територіальної цілісності України.

Законодавчі аспекти для боротьби з пропагандою війни постійно розвиваються через постанови Верховної Ради України. Вони визначають обставини та фіксують випадки пропаганди війни проти України, створюючи необхідний фундамент для притягнення винних осіб до відповідальності.

Ми розглядаємо цю практику як успішну, тому що вважаємо, що Постанови Верховної Ради України, наведені вище, є лише маленькою краплею доказів серед усіх злочинів російської армії в Україні. Це важливий інструмент протидії, який має стратегічне значення, а не просто збір фактів. Ми вважаємо цю форму інструментарію цінною, зокрема для використання у кримінально-правовому переслідуванні по причинах:

1) Постанови Верховної Ради України визначають юридичні факти і спричиняють відповідні юридичні наслідки.

2) Вони також створюють основу для подальшого розвитку нормативно-правового забезпечення окремих інструментів протидії, які не були передбачені або неможливі за чинним законодавством.

3) У додаток, шляхом регулюючої діяльності український парламент проводить досліди на певному обсязі припустимих дій у боротьбі з ворогом, який у подальшому буде впроваджений у законі.

Необхідно відзначити, що, крім прийняття Постанов, парламент повинен взятись за регулювання законодавчого забезпеченні захисту "інформаційного простору та національної безпеки України, для чого необхідною є зміна інформаційної політики шляхом доповнення законодавчої та нормативно-правової бази, а також розроблення стратегії та тактики проведення боротьби в інформаційному полі для опору агресору".

В межах такого законодавства необхідно розширювати межі допустимості доказової бази для кримінального переслідування за пропаганду війни. Прийняття законів та інших нормативно-правових актів має сприяти уточненню фактів пропаганди, виявів пропаганди в будь-яких вербальних і невербальних діях, маніпуляціях, інформаційних повідомленнях тощо [56, с. 116].

Вищевказані компоненти повинні бути визнані як пропаганда в зоні воєнних дій, визначені певнім неминучими характеристиками, але також варто встановити досить жорсткі вимоги для їх встановлення. І це є першопричиною для звернення уваги парламенту на реформування нормативно-правових актів, що вже у дії в Україні, спрямованим на боротьбу з пропагандою війни з боку росії.

Наприклад, Закон України «Про припинення дії Договору про дружбу, співробітництво і партнерство між Україною та російською федерацією» від 6 грудня 2018 року No 2643-VIII, який обгрунтовує необхідність припинення дружніх відносин з росією через її ворожість до України, зокрема через пропаганду війни.

Всі ризики та погрожування з боку рф розглядаються як засоби пропаганди війни. Другий Указ Президента України від 15 березня 2016 року під номером 96/2016 стосується Стратегії кібербезпеки України, яка забезпечує моніторинг кіберпростору з метою виявлення проявів пропаганди війни.

Методи пошуку є ефективними, оскільки вони фіксують всі дані, що використовуються для вчинення злочинних дій, навіть якщо ці дані були

змінені або трансформовані. Незважаючи на те, що параметри та вирази можуть бути відмінними та інші аспекти дозволяють зазначити, як саме конкретні користувачі інформаційних ресурсів вчиняють злочинні дії.

Слід зазначити, що для ефективної реалізації положень кримінального законодавства потрібно створити організаційно-правові механізми для виявлення фактів поширення, їх ідентифікації, фіксації, а також для розкриття виконавців і ініціаторів тощо.

Під час обговорення протидії збройному конфлікту та переслідування осіб, винних у поширенні пропаганди війни, необхідно розуміти складність ідентифікації цих осіб та доведення факту їх участі у пропагандистській діяльності.

Зокрема, в умовах правової системи України, особливо під час окупації Донбасу, іншультування певних лозунгів, висловлювань та риторики росії можуть інтерпретуватися як співзвучні звернення до забезпечення миру та захисту інтересів українських громадян.

Відповідно до національного законодавства, слід уникати таких ситуацій, оскільки кримінальне переслідування за пропаганду війни росії проти України завжди буде висвітлюватися відповідним чином у інформаційному просторі. Росія може використати цю ситуацію як елемент антидемократичних заходів, тиску чи залякування через політичні переконання, а також як частину недружньої політики українського уряду.

Боротьба з російською агресією на етапі кримінального переслідування повинна ґрунтуватися на політичній та суспільній доцільності, рівень якої наразі на досить великому рівні, а також базуватися на принципах кримінального права та кримінального правосуддя.

Таким чином, приймаючи рішення про розширення можливостей криміналізації окремих складів злочинів або дій, слід забезпечити суди доступом до доказів юридичних фактів та обставин злочинної поведінки щодо протидії пропаганді війни від росії, важливо використовувати також засоби ЄСПЛ.

Наприклад, варто згадати рішення у справі Mozer проти Республіки Молдова та росії від 23 лютого 2016 року. У цьому вироку було визнано, що було застосовано незаконні методи впливу до особи, виконані нелегітимними органами, хоча це сталося на території, яка перебуває під суверенітетом Республіки Молдова. ЄСПЛ підкреслив, що права, які гарантує Конвенція, повинні діяти згідно правил по всій Україні.

Саме через цю причину, ЄСПЛ визнав росію винною, підтвердивши, що при наданні тривалої економічної, політичної, військової та ідеологічної підтримки, Придністровська Молдавська Республіка не набуває статусу суб'єкту міжнародного права [57, с. 62-68].

Ці дії вказують на порушення основних прав та свобод людини і громадянина. Цей висновок можна застосувати до вітчизняної правової дійсності, враховуючи, що в разі прийняття подібного рішення відносно громадян України у ЄСПЛ, це рішення може бути розглянуто як приклад, коли порушено конституційні права особи.

Недотримання основних складових правового статусу людини, а також ворожі агресивні дії росії проти України, включаючи пропаганду війни, є встановленим юридичним фактом.

Така оцінка дуже спрощить процедуру кримінального переслідування осіб, винних у такому злочині. Рішення ЄСПЛ у даному випадку є лише одним прикладом в застосуванні міжнародних механізмів протидії пропаганді війни в Україні.

Проблема інформаційної війни набирає все більше популярності, оскільки це нового типу конфлікт, що спрямований на маніпулювання свідомістю людей. Інформаційна війна полягає у здатності контролювати та маніпулювати громадською свідомістю, підпорядковуючи волю людини. Цей вплив часто відбувається поза усвідомленням тих, хто піддається інформаційному впливу.

Інформаційну кампанію відрізняють такі риси, як інтенсивність, раптовість, системність, використання надмірного негативу та багату

візуалізацію. Один з ключових аспектів цього процесу - це журналісти, спеціалізовані на конкретній тематиці.

Інформаційна війна дозволяє впливати на різні соціальні, політичні та економічні процеси на всіх рівнях суспільства, даючи можливість управляти людьми та змушувати їх діяти в певний спосіб, часто на шкоду власним інтересам. Методи ведення інформаційної війни визначають способи впливу на масову свідомість та громадську думку.

Нещодавні події в сучасному світі демонструють потужність інформаційного впливу на колективну свідомість, що може мати руйнівні наслідки. Постійно з'являються купа новин, що постійно надходить від ЗМІ, часто надається з емоційним підтекстом, що може бути важко опозиції для населення.

Питання інформаційної війни стає критичним для будь-якого суспільства. При зростанні впливу ЗМІ на населення збільшується загроза негативного впливу на громадян.

Моделі, що використовуються в інформаційній війні, все частіше переплітаються, ускладнюючи розуміння населення про правду і хибу. Якщо раніше інформаційна війна була супутнім механізмом реальної війни, сьогодні вона є окремою стратегією впливу на колективну свідомість та громадську думку [58, с. 154-178].

Сучасні новини у світі підтверджують високу результативність дії інформації на глобальну людську психологію. Поміж найяскравіших зразків, що демонструють швидку зміну "інформаційної війни" за останні роки, треба впевнено заявити, що ним є конфлікт між Україною та росією.

У минулому обсяг передаваної інформації був незначним, і протистояти йому було менш складно. Проте нові технології приносять з собою величезний потік інформації, який може мати руйнівний вплив.

Інформація, яку ми отримуємо з мас-медіа, переважно впливає на наші емоції, ускладнюючи можливість опору. Цей вплив не обмежується лише

індивідуальною свідомістю, але також охоплює масову свідомість, включаючи маси нації та навіть міжнародне співтовариство [59, с. 87-92].

Наприклад, події в Україні у 2013 році, що розпочалися як мирні протести, пізніше перетворилися на жахливі та кровавi події на Майдані, та ще одну українську Революцію, яку в певній мірі підштовхувала пропагандистська інформація з росії.

Отже, значний інтенсивний вплив інформації на країну за короткий період часу увів у революцію владу у країні. Під терміном "інформаційна війна" найчастіше розуміють використання різних засобів комунікації з метою підірвання мотивації супротивника.

Інформаційна війна часто ґрунтується на моделі руйнування. Крім того, інформаційна війна може мати позитивний вплив (наприклад, прагнення покращити умови життя), але при цьому мати деструктивний характер. Часто рівень такого впливу не відповідає очікуванням населення. Результати наукових досліджень дозволяють краще зрозуміти природу і суть інформаційних конфліктів [60, с. 150-179].

ВИСНОВКИ

Згідно з наданими завданнями у ході дослідження проблематики інформаційних війн автор дійшов до таких висновків:

1. У зв'язку з актуальністю проблеми інформаційних війн, сучасна наукова спільнота приділяє збільшену увагу на дослідження даного інституту. Однак різноманіття авторських поглядів та концептуальних підходів до визначення основного змісту і видів призвело до неможливості створення єдиної дефініції інформаційної війни або уніфікованої класифікаційної структури.

Сучасний стан інформаційного законодавства України потребує негайних заходів для його вдосконалення через зростаючу видимість його недоліків. Проте серед вчених, що досліджують це питання, немає єдності щодо стратегій успішного оновлення законодавства. Ця розбіжність може бути зумовлена складністю, динамічністю та широким охопленням сучасних інформаційних процесів у контексті будівництва національної правової системи.

Інформаційна безпека охоплює заходи, спрямовані на захист інформації від несанкціонованого доступу, руйнування, зламу або розголошення. Кібербезпека зосереджується на захисті мереж, систем і даних від кіберзлочинців та кіберзагроз. Воєнний стан визначається як ситуація, коли країна знаходиться в стані війни або загрози війни, що призводить до введення спеціальних заходів для забезпечення безпеки країни.

2. Досліджено місце медіа війни в загальній системі національної безпеки України. Слід наголосити на важливості розглядати інформаційну безпеку як ключовий елемент національної безпеки держави. Ця безпека Вона відображає взаємозв'язки між інтересами індивіда, суспільства та держави в інформаційній сфері, а також правовими засобами її захисту.

Це включає рівень захищеності інформаційного простору, даних і ресурсів держави, а також інформаційної інфраструктури та телекомунікацій від потенційних загроз як зсередини, так і ззовні. Система державної інформаційної безпеки є необхідною елементом загальної системи національної безпеки держави.

Дана система налічує в собі органи державної влади, приватні структури та громадян, які спільно здійснюють заходи для забезпечення інформаційної безпеки на основі спільних правових стандартів для ефективного протистояння інформаційним загрозам у сучасних умовах. Основна мета діяльності органів державної влади полягає у виконанні конкретних завдань у цій галузі та поєднанні для забезпечення відповідних умов для досягнення цілей забезпечення інформаційної безпеки України.

3. Досліджено державну політику стосовно інформаційної безпеки. Безспірним фактом є те, що актуальні ризики медіаційній безпеці становлять виклик, який виходить за межі нашої країни і має глобальні наслідки. Для того щоб ефективно запобігти цим загрозам і реагувати на них, необхідно не лише створити відповідну нормативно-правову базу, але й забезпечити належне функціонування інституційного механізму для гарантування інформаційної безпеки, включаючи компонент освіти.

Мається на увазі скоординована діяльність державних та правових інституцій, які повинні ефективно захищати національні інтереси в інформаційній сфері, протидіяти поширенню фейків та дезінформації, а також запобігати виникненню різних суперечок та сприяти формуванню інформаційної культури суспільства.

Ураховуючи також наявні глобальні загрози та виклики, здається можливою ефективна боротьба з інформаційною агресією за допомогою залучення міжнародних організацій, інституцій та міжнародної спільноти до цього процесу. В наш час ведення війни в інформаційному просторі не зазнає жодних обмежень.

4. Проаналізовано законодавче забезпечення інформаційної безпеки в Україні. Юридичне забезпечення інформаційної безпеки в Україні має велике значення у забезпеченні захисту цифрових даних, протидії кіберзлочинності та збереженні приватності громадян. В країні діє ряд законів, які регулюють цю сферу, такі як Закон "Про захист персональних даних", Закон "Про кібербезпеку" та інші. Висновок полягає в тому, що в Україні існують відповідні правові норми для забезпечення інформаційної безпеки, але важливо постійно вдосконалювати їх у відповідь на зростаючі виклики у сфері кібербезпеки.

5. Інноваційні методи забезпечення інформаційної безпеки є ключовим елементом сучасних стратегій кіберзахисту. Вони багаторазово підтвердили свою ефективність у запобіганні кіберзлочинності та захисті конфіденційності даних.

Шляхом впровадження інноваційних підходів, організації можуть підвищити рівень захисту своєї інформації, реагувати на загрози в реальному часі та забезпечити стійкість своєї інфраструктури до потенційних атак. Висновок полягає в тому, що інноваційні методи забезпечення інформаційної безпеки є необхідними для успішного функціонування сучасних систем, що працюють з великим обсягом даних.

6. Застосування кіберзаходів та кіберзахисту в Україні відображає важливість забезпечення кібербезпеки у державі. В останні роки, Україна активно вдосконалює свої кіберзаходи та кіберзахист з метою захисту від кібератак та злочинів у кіберпросторі. Ці заходи важливі для ефективного функціонування державних установ, захисту конфіденційної інформації та забезпечення безпеки громадян. Досягнення в цій сфері сприяють підвищенню захищеності країни в інформаційному просторі та підтримують її національну безпеку.

7. Проаналізовано особливості впливу воєнного стану на інформаційну безпеку в Україні. По-перше, воєнний стан може призвести до збільшення поширення дезінформації та фейків, що загрожує надійності та достовірності

інформації. За таких умов громадяни можуть стати жертвами маніпуляцій та пропаганди.

По-друге, воєнний стан може призвести до обмежень у доступі до інформації, що може суттєво обмежити свободу слова та право на отримання надійної інформації для громадян.

По-третє, воєнний стан може призвести до зростання кіберзлочинності та кібератак, що загрожує кібербезпеці та цілісності інформаційних систем.

Загалом, вплив воєнного стану на інформаційну безпеку в Україні є значний і вимагає комплексних заходів забезпечення безпеки та надійності інформації в умовах конфлікту.

8. Здійснено аналіз місця і ролі інформаційної війни та пропаганди в контексті воєнного стану. Роль інформаційної війни та пропаганди в контексті воєнного стану не може бути недооцінена. Інформаційна війна займає особливе місце на думку громадськості, мобілізації суспільства та формування образу ворога.

Пропаганда в цьому контексті використовується для поширення спроможностей власної сторони та дискредитації противника. Ефективність інформаційної війни та пропаганди в значній мірі залежить від якості та об'єму інформації, що надається, а також від рівня доступності до цієї інформації. У контексті воєнного стану важливо мати різноманітні джерела інформації та критично оцінювати їх для уникнення маніпуляцій та запобігання впливу пропаганди на прийняття важливих рішень.

9. Міжнародний досвід та кращі практики у сфері інформаційної безпеки під час воєнного стану відіграють критичну роль у забезпеченні захисту країни та її громадян в умовах конфлікту. Оптимальне використання новітніх технологій та ретельне планування заходів забезпечення кібербезпеки можуть значно зменшити ризики для інформаційних систем і даних під час військових дій. Співпраця між країнами та використання найкращих практик у цій галузі є ключовими елементами ефективного відстоювання від кіберзагроз у період воєнного стану.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пунда О.О., Добрянська О.Д., Новицька Н.Б. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. *Екологічне право.* 2022. № 1-2. С. 60–61

2. Новицький А. Щодо питання структуризації інформаційного права як наукової категорії. *Актуальні проблеми правознавства*. 2016. Вип. 4. С. 34–38.

3. Новицька Н.Б. Захист суспільної моралі в інформаційному суспільстві. Інформація і право. 2011. No 3(3). С. 28–33.

4. Цимбалюк В. Інформаційне право (основи теорії і практики): моногр. К. : «Освіта України», 2010. 388 с.

5.Основи інформаційного права України: навч. посіб. В. Цимбалюк, В. Гавловський, В. Брижко. К. : Знання, 2009. 414 с.

6. Селезньова О. Теоретико-методологічні основи інформаційного права України : моногр. Чернівці: *Місто*, 2014. 408 с.

7. Заніздра Н. О. Державна інформаційна політика на сучасному етапі та шляхи вдосконалення. *Вісник КрНУ імені Михайла Остроградського*. 2012. № 2. С. 193–196.

8. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2020. Т. 7. No2. С. 56–61.

9. Про інформацію : Закон України від 2 жовтня 1992 р. No 2657-XII. URL. https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 20.01.2025 р.)

10. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. No 2657-XII. URL. https://zakon.rada.gov.ua/laws/ show/2939-17. (дата звернення 20.01.2025 р.)

11. Про основні засади забезпечення кібербезпеки України : Закон України від 9 травня 2018 р. No 2163-VIII. URL. https://zakon.rada.gov.ua/laws/show/2163-19/

12. Про боротьбу з тероризмом : Закон України від 20 березня 2003 р. No 638-IV. URL. https://zakon.rada.gov.ua/laws/show/638-15

13. Про введення воєнного стану в Україні : Указ Президента України від 24 лютого 2022 року No64/2022 URL: https://www.president.gov.ua/documents/642022-41397

14. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної полі- тики в умовах воєнного стану»: Указ Президента України URL: https://www.president.gov.ua/documents/1522022-41761.

15. Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану : Наказ Головнокомандувача Збройних Сил України від 03 березня 2022 року No73. URL. https://www.mil.gov.ua/content/mou_orders/nakaz_73_050322.pdf?fbclid=IwAR3BFiXuFblkYZgRCWVYGHffTJhtmhBbQXAEVE7

16. Про медіа : Закон України від 13 грудня 2022 року No 2849-IX. Законодавство України. Верховна Рада України. URL. https://zakon.rada.gov.ua/laws/show/2849-20#Text/.

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

18. Зубок М.І. Інформаційна безпека: навч. Посібник. М.І. Зубок; Київський національний торговельно-економічний ун-т. – К. : КНТЕУ, 2005. – 133.

19. О.Г. Трофименко Законодавча база забезпечення кібербезпеки держави. *Кібербезпека в Україні: правові та організаційні питання*: матер. II всеукр. наук.-практ. конф., 17 листопада 2017 р., Одеса: ОДУВС, С. 55–56.

20. О. Трофименко, Я. Дубовой, "Щодо правового потенціалу безпечного функціонування кіберпростору", *Кібербезпека в Україні: правові та організаційні питання:* матер. III всеукраїнської наук.-практ. конф., 30 листопада 2018 р., Одеса: ОДУВС, С. 5–7.

21. Д. Безуглий, "Інформаційна безпека України: огляд останніх тенденцій", *Фізико-математична освіта*, вип. 2(16), с. 13–17, 2018.

22. Впровадження європейської кібербезпеки: загальний огляд. ISACA. URL: https://www.isaca.org/Knowledge-Center

23. Вовканич Д. М. Правове забезпечення інформаційної безпеки в умовах гібридної війни: thesis. 2020. URL: https://er.nau.edu.ua/handle/NAU/44837

24. Radzyvyliuk Y. Особливості убезпечення інформаційного простору Італії в контексті розвитку інформаційно- комунікативних технологій. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2020. № 1 (7). С. 112–122.

25. Nofenko A. Гібридна війна росії проти України: інформаційний наступ та механізми протидії. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2019. № 2 (6). С. 68–77

26. Nashynets-Naumova A. Y. Правове забезпечення інформаційної безпеки в закладах вищої освіти україни. *Modern achievements of eu countries and ukraine in the area of law*. 2020. P. 376–388.

27. Fedorova H. Нормативно-правове регулювання питань забезпечення безпечного середовища для життя громадян. *Public administration and regional development*. 2019. № 3. С. 162–177.

28. Chumak D., Klevtsov O. Комп‘ютерна безпека на ядерних об’єктах в Україні. *Nuclear and radiation safety*. 2015. № 3(67). С. 328

29. Шемчук В. Принципи забезпечення інформаційної безпеки. *Наукові записки інституту законодавства верховної ради україни*. 2018. № 4. С. 50–56.

30. Федоренко А. Є. Стратегія забезпечення розвитку інформаційної сфери економіки України: thesis. 2020. URL:http://ir.stu.cn.ua/123456789/20457

31. Рогова Є. І. Теоретичні основи правового забезпечення інформаційної безпеки. *Актуальні проблеми держави і права*. 2020. № 86. С. 190–196

32. Савінова Н. А., Savinova N. A. Кримінально-правова політика забезпечення інформаційного суспільства в Україні: дисертація : thesis. 2013. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/788

33. Шемчук В. В. Економічна та інформаційна безпека держави: правові аспекти співвідношення. *Актуальні проблеми держави і права*. 2020. № 83. С. 253–259

34. Перун Т. Структурні чинники механізму інформаційної безпеки держави. *Юридичний вісник*. 2020. № 4. С. 117–124.

35. Лукаш В. О. Правове забезпеченя інформаційної безпеки в цивільній авіації : thesis. 2014. URL: http://er.nau.edu.ua/handle/NAU/12741

36. Кунєв Ю. Д., Легеза Є. О. Правове забезпечення інформаційної безпеки як предмет адміністративно-правового дослідження : thesis. 2021. URL: https://er.nau.edu.ua/handle/NAU/48701

37. Калетнік В. В. Сучасний стан адміністративно-правового забезпечення інформаційної безпеки в Україні: теоретико-правовий аналіз : thesis. 2021. URL: https://er.nau.edu.ua/handle/NAU/53718

38. Про основні засади забезпечення кібербезпеки України: Закон України. *Урядовий кур'єр*, № 215, 2017.

39. Кутрова Г. В. Міжнародно-правові стандарти регулювання правил екологічної безпеки: магістерська робота. 2020. URL: https://dspace.znu.edu.ua/jspui/handle/12345/2519

40. Перун Т. С. Забезпечення інформаційної безпеки в зоні бойового конфлікту. *Актуальні проблеми держави і права*. 2020. № 87. С. 131–138

41. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник. К.: КНТ, 2010. 776 с.

42. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с

43. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року No 47/2017 URL: https://zakon.rada.gov.ua/go/47/2017.

44. Боднар І. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки.* 2014. No 1. С. 68–75.

45. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету. Право.* № 77. 2023, с. 121-128

46. Стадник А. Г. Основні моделі організації інформаційних війн та їх різновиди. *Соціальні технології: актуальні проблеми теорії та практики,* 2015, №. 67–68, с. 81-85

47. Коруц У. Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. Підприємництво, господарство і право. № 8. 2020, с. 334-338

48. Семен Н. Ф. російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог»): ареф. дис. к. н. соц. комун; спеціальність 27.00.01. Дніпро: Дніпровський національний університет імені Олеся Гончара, 2018. 23 с.

49. Малик Я. Інформаційна війна і Україна. *Науковий вісник*. 2015. Вип. 15. URL : http:// www.lvivacademy.com/vidavnitstvo_1/visnyk15/ fail/Malyk.pdf.

50. Андрєєва О. М. Інформаційна безпека України як чинник міжнародної інформаційної безпеки. *Вісник Київського національного*

університету імені Тараса Шевченка. Міжнародні відносини. 2004. Вип. 29/30. С. 67–69.

51. Бартош Н. В. Актуальні питання удосконалення реалізації державної інформаційної політики україни в умовах гібридної війни. *Public management.* 2022. Т. 28, № 3. С. 17–24.

52. Батечко О., Цимбаленко Н. В. Інформаційна безпека підприємства : thesis. 2016. URL: https://er.knutd.edu.ua/handle/123456789/4464

53. Бєльська Т., Лашкіна М., Нестеряк Ю. Інформаційна політика та інформаційна безпека держави як психосоціальне явище: проблеми та перспективи. *Public management.* 2020. Т. 22, № 2. С. 119–132.

54. Боднар І. Р. Заходи держави в сфері інформаційної безпеки. *Herald of lviv university of trade and economics economic sciences*. 2020. № 59. С. 37–41.

55. Войтюк Л. М. Інформаційна безпека праці державних службовців: теоретико-правові аспекти. *Знання європейського права*. 2020. № 2. С. 31–35.

56. Дослідження моделі міжнародного інформаційного простору з метою пошуку ефективних механізмів захисту національного інформаційного суверенітету / O. Serpukhov та ін. *Системи управління, навігації та зв'язку. Збірник наукових праць.* 2018. Т. 6, № 52. С. 116–121.

57. Корнієнко О. В. Інформаційна безпека особистості як передумова підтримання психосоматичного здоров'я молоді. *Problems of modern psychology*. 2022. № 4. С. 62–68.

58. Лисенко С. Сучасні тенденції розвитку інформаційної безпеки як об'єкта правовідносин. *Public management*. 2019. Т. 17, № 2. С. 154–173.

59. Младьонова О. Д. Інформаційна безпека як складова національної безпеки України. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія "Питання політології"*. 2017. Вип. 31. С. 87–92.

60. Новородовський В. Інформаційна безпека України в умовах російської агресії. *Society. Document. Communication.* 2020. № 9. С. 150–179